DOI: 10.18137/RNU.V9187.22.02.P.052 УДК 004.056.53

Г.И. Бахрушина, Т.В. Жукова, А.Е. Утюпин

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ ОБРАТИМОГО АЛГОРИТМА СОКРЫТИЯ ДАННЫХ В ЗАШИФРОВАННЫХ ИЗОБРАЖЕНИЯХ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ КОДА ХЭММИНГА (7,4) И MSB-ПРОГНОЗИРОВАНИЯ[1]

Аннотация. Приводятся результаты экспериментального исследования обратимого алгоритма сокрытия данных в зашифрованных изображениях, использующего код Хэмминга (7,4) и MSB-прогнозирования, который был разработан на основе алгоритма китайских исследователей Каймен Чена и Чин-Чен Чанга и реализован на языке программирования C#.

Ключевые слова: цифровое изображение, полутоновое изображение, код Хэмминга, цифровое маркирование изображения, секретное сообщение, MSB-прогнозирование, обратимый алгоритм, пиковое отношение сигнал/шум, нормализованный коэффициент корреляции, порог внедрения.

G.I. Bakhrushina, T.V. Zhukova, A.E. Utjupin

EXPERIMENTAL STUDY OF THE REVERSIBLE ALGORITHM FOR HIDING DATA IN ENCRYPTED IMAGES BASED ON THE USE OF (7,4) HAMMING CODE AND MSB PREDICTION

Abstract. The article presents the results of an experimental study of one reversible algorithm for hiding data in encrypted images using (7,4) Hamming code and MSB prediction, which was developed based on the algorithm of Chinese researchers Kaimeng Chen and Chin-Chen Chang and implemented in the C# programming language.

Keywords: digital image, grayscale image, Hamming code, digital image marking, secret message, MSB prediction, reversible algorithm, peak signal-to-noise ratio, normalized correlation coefficient, embedding threshold.

Введение

На сегодняшний день известен и исследован ряд методов обратимого сокрытия данных, которые работают с изображениями. В основном эти методы используют расширение разницы (DE) [7], сдвиг гистограммы (HS) [8], упорядочивание значений пикселей (PVO) [3; 6] и модификацию ошибок прогнозирования [2; 4; 5]. Все эти методы учитывают пространственную корреляцию и избыточность изображений для встраивания дополнительных битов.

Алгоритм, рассматриваемый в данной работе, был представлен китайскими учеными Каймен Ченом (Kaimeng Chen) и Чин-Чен Чангом (Chin-Chen Chang) в статье [4]. Он основан на кодировании по Хэммингу (7,4) и MSB-прогнозировании.

[1] Работа выполнена в Дальневосточном центре математических исследований при финансовой поддержке Минобрнауки России, соглашение от 4 февраля 2022 г. № 075-02-2022-879 по реализации программ развития региональных научно-образовательных математических центров.

Бахрушина Галина Ивановна
кандидат физико-математических наук, доцент, доцент кафедры программного обеспечения вычислительной техники и автоматизированных систем. Тихоокеанский государственный университет, город Хабаровск. Сфера научных интересов: информационные технологии; разработка программного обеспечения; цифровое маркирование изображений. Автор более 70 опубликованных научных работ.
Электронный адрес: gal_bah@mail.ru

Жукова Татьяна Витальевна
старший преподаватель кафедры программного обеспечения вычислительной техники и автоматизированных систем. Тихоокеанский государственный университет, город Хабаровск. Сфера научных интересов: информационные технологии; разработка программного обеспечения; цифровое маркирование изображений. Автор более 10 опубликованных научных работ.
Электронный адрес: 000521@pnu.edu.ru

Утюпин Артем Евгеньевич
магистрант по направлению подготовки «Программная инженерия». Тихоокеанский государственный университет, город Хабаровск. Сфера научных интересов: информационные технологии; разработка программного обеспечения. Автор 3 опубликованных научных работ.
Электронный адрес: 2017103156@pnu.edu.ru

Ранее авторами была подготовлена и опубликована статья [1] с детальным описанием вышеуказанного алгоритма, реализованного на языке C#. В настоящей статье приводятся результаты экспериментального исследования алгоритма.

Метрики, позволяющие измерять эффективность алгоритма

Для измерения эффективности алгоритма в работе использовались такие известные метрики, как PSNR, NC и BPP.

Пиковое отношение сигнала к шуму (PSNR). PSNR (Peak Signalto Noise Ratio) используется для измерения уровня искажений при работе с изображениями. PSNR отражает соотношение между максимумом возможного значения сигнала и мощностью шума, искажающего значение сигнала. Обычно измеряется в децибелах (при полном совпадении изображений PSNR стремится к бесконечности). Для его определения используется среднеквадратичная ошибка MSE (Mean Square Error).

Для двух изображений I и K размером $m \times n$, одно из которых считается зашумленным приближением другого, MSE вычисляется по формуле

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \left| I(i,j) - K(i,j) \right|^2 ; \quad (1)$$

PSNR определяется по формуле

$$\text{PSNR} = 10 \log_{10} \left(\frac{MAX_I^2}{MSE} \right), \quad (2)$$

где $MAX_I = 255$ для разрядности 8 бит или максимальному значению, принимаемому пикселем изображения, – в противном случае.

Считается, что человеческий глаз практически не различает искажений при PSNR $\geq 35 дБ$.

Коэффициент нормированной взаимной корреляции (NC). NC используется в качестве меры идентичности исходного и маркированного изображения или для сравнения внедренной и извлеченной информации.

Для двух изображений I и K размером $m \times n$ NC вычисляется по формуле

$$NC = \frac{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} I(i,j)K(i,j)}{\sqrt{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} I(i,j)^2 \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} K(i,j)^2}}. \quad (3)$$

Значения коэффициента находятся в диапазоне $[0, 1]$. Чем ближе коэффициент к единице, тем больше сходство между сравниваемыми изображениями (при полном совпадении изображений NC равно единице).

Порог внедрения (ER). ER (Embedding Rate) – максимальное количество бит, которое можно внедрить в один пиксель изображения с помощью рассматриваемого алгоритма. Рассчитывается как отношение максимально возможного объема внедрения в изображение к общему числу пикселей изображения. Единица измерения – количество бит на пиксель, или bpp (bit per pixel). Для данного алгоритма порог внедрения определяется по формуле

$$ER = \frac{3}{7} \cdot \frac{(m-2)(n-2)}{mn}, \quad (4)$$

где m и n – размеры изображения.

Результаты экспериментальных исследований

Для экспериментальных исследований было выбрано 15 изображений разных размеров (Grapes, Lynx и Safari размером 128×128 пикселей, Cameraman, Bird, Barbara – 256×256, Baboon, Lena, Jet – 512×512, Road, Car, Leopard – 800×600, Boeing, Smoke, Good Day – 1000×1000).

Были изучены следующие зависимости:

– качество внедрения короткого и длинного сообщения от размера изображений;

– значение порога внедрения от размера изображения.

Зависимость качества внедрения длинного сообщения от размера изображений. На Рисунках 1, 2 представлены исходные и маркированные изображения Grapes, Lynx и Safari размером 128×128 пикселей, а в Таблице 1 отражены значения метрик PSNR и NC между исходными и соответствующими маркированными изображениями для случая внедрения длинного сообщения. Длинное сообщение считывается из текстового файла (см. Рисунок 3).

Рисунок 1. Исходные изображения размером 128×128

Рисунок 2. Маркированные изображения размером 128×128 с внедренным длинным сообщением

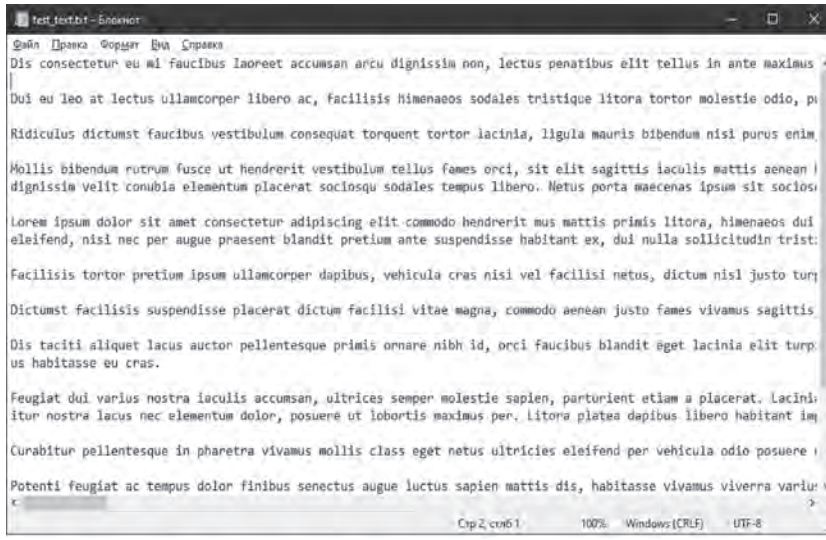

Рисунок 3. Текстовый файл test_text.txt с длинным сообщением

Таблица 1

Значения метрик PSNR и NC при внедрении длинного сообщения для изображений размером 128×128

Изображение	PSNR	NC
Grapes	46,4027069396312	0,999955883479634
Lynx	50,9078554195244	0,999970363034833
Safari	50,9274942550007	0,999981930509711
Среднее значение	49,4126855380521	0,999969392341393

В Таблицах 2–5 приведены значения метрик PSNR и NC для исходных и соответствующих им маркированных изображений остальных фиксированных размеров при внедрении длинного сообщения, а также их средние значения.

Таблица 2

Значения метрик PSNR и NC при внедрении длинного сообщения для изображений размером 256×256

Изображение	PSNR	NC
Bird	50,8130603552931	0,999983178209008
Cameraman	46,2522171826809	0,999957147093394
Barbara	44,5285277171326	0,999912319764618
Среднее значение	47,1979350850355	0,999950881689007

Таблица 3

Значения метрик PSNR и NC при внедрении длинного сообщения для изображений размером 512×512

Изображение	PSNR	NC
Baboon	48,8691370155287	0,999978767213198
Lena	50,7906899463369	0,999984670519845
Jet	50,8102654203584	0,999992211553999
Среднее значение	50,1566974607413	0,999985216429014

Таблица 4

Значения метрик PSNR и NC при внедрении длинного сообщения для изображений размером 800×600

Изображение	PSNR	NC
Road	50,5264531123524	0,999983509465575
Car	45,4008487943587	0,999949281192931
Leopard	48,2014871202226	0,999954377327815
Среднее значение	48,0429296756446	0,999962389328774

Таблица 5

Значения метрик PSNR и NC при внедрении длинного сообщения для изображений размером 1000×1000

Изображение	PSNR	NC
Boeing	47,8585351470399	0,999976216816141
Smoke	48,4735810088247	0,999917503500045
GoodDay	50,7789359775193	0,999982467304119
Среднее значение	49,0370173777946	0,999958729206768

На Рисунках 4, 5 представлены графики зависимости значения метрик PSNR и NC соответственно, построенные по средним значениям из Таблиц 1–5.

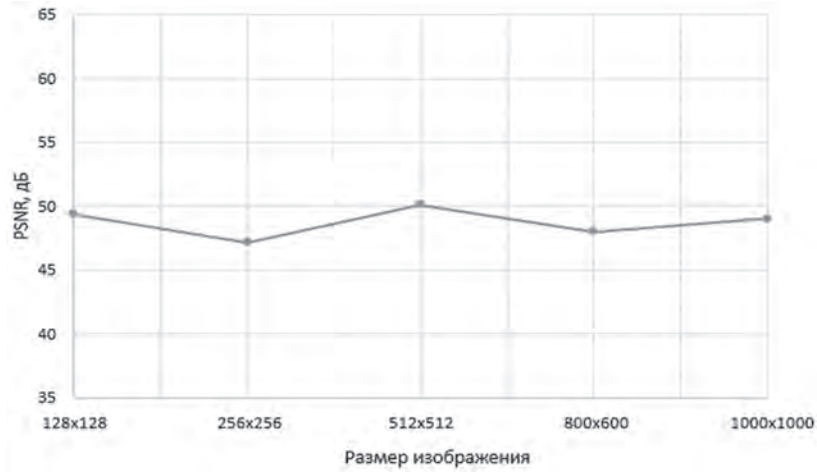

Рисунок 4. График зависимости значения метрики PSNR от размеров изображений при внедрении длинного сообщения

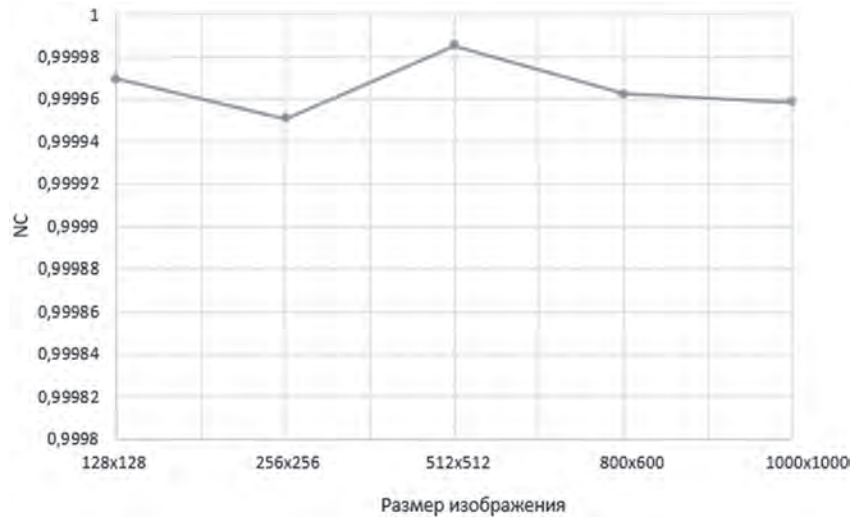

Рисунок 5. График зависимости значения метрики NC от размеров изображений при внедрении длинного сообщения

Установлено, что значения PSNR колеблются в пределах примерно от 45 до 50 дБ, что является хорошим показателем. Во всех случаях разница изображений незаметна для глаз. Значения NC приближены к единице, следовательно, изображения очень похожи. В целом зависимость значений метрик от размера изображения выражена очень слабо – практически не просматривается (наблюдаются лишь небольшие колебания значений метрик). Возможно, получить более точный результат удалось бы при наборе большей статистики.

Внедрение короткого сообщения. Аналогичные исследования были выполнены для случая внедрения короткого сообщения. Короткое сообщение задается в программе строкой Hello, World! При внедрении короткого сообщения показатели качества внедре-

ния несколько выше – значение PSNR колеблется в пределах примерно от 55 до 60 дБ, а значения NC либо равны единице, либо близки к ней. Зависимость значений метрик от размера изображения также слабо выражена (но показатели несколько выше для изображений небольшого размера).

Зависимость значения порога внедрения от размера изображения. Для расчета порога внедрения использовалась формула (4). В Таблице 6 приведены данные расчета порога внедрения для изображений разных размеров.

Таблица 6

Данные расчета порога внедрения для изображений разных размеров

Размер изображения	Порог внедрения
128×128	0,415283203
256×256	0,421890259
512×512	0,425228119
800×600	0,426075000
1000×1000	0,426858000

На Рисунке 6 представлен график зависимости порога внедрения от размера изображения.

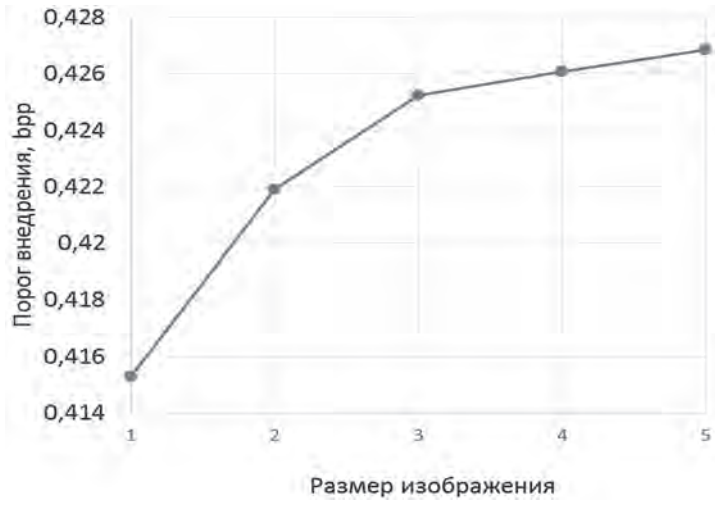

Рисунок 6. График зависимости порога внедрения от размера изображения: *1* – изображение размером 128×128; *2* – 256×256; *3* – 512×512; *4* – 800×600; *5* – 1000×1000

Из графика видно, что порог внедрения ER растет при увеличении размера изображения. Это можно объяснить тем, что при увеличении размера изображения растет число модифицируемых пикселей.

Заключение

Рассмотренный алгоритм был реализован на языке программирования C# в среде разработки Microsoft Visual Studio 2019 и исследован на обратимость, качество встраивания и извлечения информации. С помощью разработанной программы была исследована за-

висимость основных метрик, характеризующих эффективность алгоритма (PSNR и NC), а также порога внедрения (ER) от размера изображения. При этом рассматривались короткие и длинные внедряемые сообщения.

При выполнении экспериментальных исследований было установлено, что PSNR между исходным и маркированным изображениями находится на высоком уровне (от 45 до 60 дБ).

Литература

1. *Бахрушина Г. И., Жукова Т. В., Утюпин А. Е.* Обратимый алгоритм сокрытия данных в зашифрованных изображениях, использующих код Хэмминга (7, 4) и MSB-прогнозирование // Вестник ТОГУ. 2022. № 1 (64). С. 55–64.

2. *Aswathy Lekshmi S., Hari S., Netha Merin Mathew* (2019) High Capacity Reversible Data Hiding in Encrypted Images by MSB Prediction Method. International Research Journal of Engineering and Technology (IRJET), vol. 06, Iss. 04.

3. *Chin-Feng Lee, Jau-JiShen, Yu-Chi Kao* (2018) High-Capacity Reversible Data Hiding Based on Star-Shaped PVO Method. Recent Advances in Intelligent Information Hiding and Multimedia Signal Processing, vol. 109.

4. *Kaimeng Chen, Chin-Chen Chang* (2019) Real-Time Error-Free Reversible Data Hiding in Encrypted Images Using (7, 4) Hamming Code and Most Significant Bit Prediction. Symmetry, vol. 11. Available at: https://doi.org/10.3390/sym11010051 (date of the application: 28.04.2021).

5. *Pauline Puteaux, William Puech* (2018) An Efficient MSB Prediction-Based Method for High-Capacity Reversible Data Hiding in Encrypted Images. IEEE Transactions on Information Forensics and Security, vol. 13 (7), pp. 1670–1681. doi: 10.1109/TIFS.2018.2799381

6. *Qu X., Kim H. J.* (2015) Pixel-based pixel value ordering predictor for high-fidelity reversible data hiding. Signal Process, pp. 249–260.

7. *Tian Jun* (2003) Reversible data embedding using a difference expansion. IEEE Transactions on Circuits and Systems for Video Technology, vol. 13, Iss. 8.

8. *Zhicheng Ni, Yun-Qing Shi, N. Ansari, Wei Su* (2006) Reversible data hiding. IEEE Transactions on Circuits and Systems for Video Technology, vol. 16, Iss. 3.

References

1. Bahrushina G.I., Zhukova T.V., Utyupin A.E. (2022) *Obratimyj algoritm sokrytiya dannyh v zashifrovannyh izobrazheniyah, ispol'zuyushchih kod Hemminga (7,4) i MSB-prognozirovanie* [Reversible Algorithm for Hiding Data in Encrypted Images Using Hamming Code (7, 4) and MSB Prediction]. *Vestnik TOGU*, No. 1 (64), pp. 55–64 (in Russian).

2. Aswathy Lekshmi S., Hari S., Netha Merin Mathew (2019) High Capacity Reversible Data Hiding in Encrypted Images by MSB Prediction Method. International Research Journal of Engineering and Technology (IRJET), vol. 06, Iss. 04.

3. Chin-Feng Lee, Jau-JiShen, Yu-Chi Kao (2018) High-Capacity Reversible Data Hiding Based on Star-Shaped PVO Method. Recent Advances in Intelligent Information Hiding and Multimedia Signal Processing, vol. 109.

4. Kaimeng Chen, Chin-Chen Chang (2019) Real-Time Error-Free Reversible Data Hiding in Encrypted Images Using (7, 4) Hamming Code and Most Significant Bit Prediction. Symmetry, vol. 11. Available at: https://doi.org/10.3390/sym11010051 (date of the application: 28.04.2021).

5. Pauline Puteaux, William Puech (2018) An Efficient MSB Prediction-Based Method for High-Capacity Reversible Data Hiding in Encrypted Images. IEEE Transactions on Information Forensics and Security, vol. 13 (7), pp. 1670–1681. doi: 10.1109/TIFS.2018.2799381
6. Qu X., Kim H. J. (2015) Pixel-based pixel value ordering predictor for high-fidelity reversible data hiding. Signal Process, pp. 249–260.
7. Tian Jun (2003) Reversible data embedding using a difference expansion. IEEE Transactions on Circuits and Systems for Video Technology, vol. 13, Iss. 8.
8. Zhicheng Ni, Yun-Qing Shi, N. Ansari, Wei Su (2006) Reversible data hiding. IEEE Transactions on Circuits and Systems for Video Technology, vol. 16, Iss. 3.