



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала: <http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.056.55

СТЕГАНОГРАФИЧЕСКИЙ МЕТОД BCES ВСТРАИВАНИЯ ИНФОРМАЦИИ В РАСТРОВЫЕ ФАЙЛЫ

Мерзлякова Е.Ю.

ФГБОУ ВО "СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ", Новосибирск, Россия,
(630102, Новосибирская область, город Новосибирск, ул. Кирова, д. 86), e-mail:
katerina.artist@yandex.ru

Представлен стеганографический метод встраивания информации в файлы формата bmp на основе алгоритма интерполяции изображений. Выполнен анализ разработанного метода BCES по разностным показателям искажения и проведено сравнение с похожими методами. Рассмотренный стегометод BCES имеет ёмкость 0.5 bpp и может применяться в области защиты пользовательских данных.

Ключевые слова: Стеганография, цифровые изображения, встраивание информации, интерполяция, искажения.

THE BCES STEGANOGRAPHIC METHOD OF EMBEDDING INFORMATION IN RASTER FILES

Merzlyakova E.Yu.

SIBERIAN STATE UNIVERSITY OF TELECOMMUNICATIONS AND INFORMATICS, Novosibirsk,
Russia, (630102, Novosibirsk region, Novosibirsk, Kirova street, 86), e-mail:
katerina.artist@yandex.ru

Steganographic method for embedding information into bmp files based on an image interpolation algorithm is presented. The developed BCES method was analyzed using difference distortion indicators and compared with similar methods. The considered BCES stegomethod has capacity of 0.5 bpp and can be used in the field of protecting user data.

Keywords: Steganography, digital images, information embedding, interpolation, distortion.

Введение

Стеганография цифровых изображений является отдельной актуальной областью исследований в компьютерной стеганографии. Роль контейнера, в который встраивается информация, часто выполняют растровые файлы. Особенность таких файлов том, что можно легко заменить младшие биты без видимых искажений изображения. На данной особенности основано большинство стеганографических алгоритмов [1]. С целью улучшения безопасности в таких стегосистемах применяют также криптографические алгоритмы защиты информации [2], а для повышения качества контейнера часто используются методы интерполяции [3-8], что позволяет затем восстановить исходный (cover) контейнер. Для оценки качества стегосистем, в том числе основанных на интерполяции, используют два основных показателя: объем встроенной информации (BPP) и мера искажения изображения, выраженная в максимальном

(пиковом) соотношении сигнала к шуму (PSNR). Также иногда применяются показатель искажений (AD) и качества (IF). Цель представленной работы состоит в том, чтобы разработать метод встраивания информации в контейнеры формата bmp, применяя алгоритм интерполяции, а также исследовать полученную стегосистему в отношении возникающих искажений при встраивании.

Разработка и реализация метода BCES

Рассмотрим исходный контейнер C , представляющий собой 8-битный файл формата bmp размером 225 точек по высоте и 225 по ширине. Каждой точке соответствуют значения яркостей RGB — красного (R), зелёного (G) и синего (B) цвета. Для экспериментов при разработке стеганографических методов встраивания информации в изображения обычно используют изображения в градациях серого, когда каждый пиксель имеет равные значения яркостей для всех составляющих. Также полученные результаты действительны и для других схожих форматов с неискажающими методами сжатия, например png.

Применение метода интерполяции позволяет увеличить исходный контейнер C , добавив в него дополнительные пиксели, которые удобно использовать для встраивания данных. В методе BCES изображение увеличивается по строкам и столбцам посредством интерполяции Лагранжа, как наиболее оптимального метода получения контейнера для встраивания с использованием алгоритмов интерполяции [9]. Таким образом, размер интерполированного контейнера в данном случае составит 450 на 450 пикселей, то есть увеличится в 2 раза по сравнению с исходным. Информация будет записываться только в интерполированные значения, поэтому мы всегда можем восстановить исходное изображение C . Контейнер, полученный в результате работы стегометода называется стегоконтейнером S .

В качестве сообщения для встраивания используется двоичная псевдослучайная последовательность. Предполагается, что для повышения защиты встраиваемой информации будет использован секретный ключ, полученный, например, с помощью шифра Вернама.

Итак, возьмем интерполированный контейнер и рассмотрим значения пикселей как точки некоторой кривой. Воспользуемся формулой кривой Безье [10], чтобы построить более гладкую кривую по заданным точкам изображения. Оптимально использовать 5 точек для построения кривой по формуле (1):

$$P(t) = \sum_{i=0}^n P_i \cdot \frac{n!}{i!(n-i)!} \cdot (1-t)^{n-i} \cdot t^i, \quad (1)$$

$n=4$ для пяти точек, i – номер опорной точки;

$P(t)$ – ордината опорной точки кривой Безье;

P_i – значение цвета пикселя изображения,

$t \in [0,1]$ – заданный шаг.

Таким образом, будем рассматривать значения точек контейнера блоками по 5 пикселей, соответственно формуле (1). В каждом таком блоке три пикселя являются оригинальными опорными точками интерполяции и составляют исходную матрицу изображения до ее увеличения. Остальные точки каждого блока вычислены по алгоритму интерполяции и могут быть заменены на другие значения точек построенной кривой. Количество всевозможных точек регулируется параметром t , который может принимать значения 0,1 или меньше. Если мы хотим получить больше точек, то соответственно, нужно задать меньшее значение t . В итоге значения точек кривой в каждом блоке из пяти точек вычисляются по формуле (2):

$$P = (1 - t)^4 \cdot P_0 + 4 \cdot (1 - t)^3 \cdot t \cdot P_1 + 6 \cdot (1 - t)^2 \cdot t^2 \cdot P_2 + 4 \cdot (1 - t) \cdot t^3 \cdot P_3 + t^4 \cdot P_4. \quad (2)$$

Так как точки изображения рассматриваются подобно непрерывному сигналу, то каждая последняя точка P_4 в блоке должна являться первой точкой P_0 следующего блока.

Рассмотрим более подробно реализацию алгоритма встраивания BCES (Bezier Curves Embedding Strategy). Интерполированный контейнер рассматривается блоками из пяти значений яркости пикселей: $(P_0, P_1, P_2, P_3, P_4)$, где точки P_0, P_2, P_4 являются значениями точек исходного изображения S , а значения P_1 и P_3 являются добавленными точками соответственно выбранному алгоритму интерполяции. Обозначим значения точек кривой Безье, вычисленных между P_0 и P_2 множеством $R_1 = \{r_1, \dots, r_k\}$, а между P_2 и P_4 – множеством $R_3 = \{r_1, \dots, r_k\}$, где k – это количество значений при данном шаге t . Если рассматривать график кривой, проходящей от точки P_0 до точки P_4 , то количество отрезков на ней и является значением k , исключая первый и последний отрезок, а также два отрезка, которые окружают значение кривой, соответствующей P_2 . Таким образом, k вычисляется по следующей формуле:

$$k = \frac{1}{2-t} - 1, \quad (3)$$

Множество значений из R_1 будут использованы для замены значения точки P_1 , а множество значений из R_3 соответственно для замены P_3 . Значения точек кривой, соответствующие P_0, P_2 и P_4 не используются для замены значений P_1 и P_3 , так как они являются пикселями изображения S . Если встраивать один бит информации в каждую подходящую точку изображения, то в данном алгоритме количество встроенных бит составит половину от общего числа точек всего изображения S , так как рассматриваемые блоки точек пересекаются в крайнем их значении.

Рассмотрим график кривой Безье, построенной по усредненным значениям яркостей пикселей с шагом $t=0.1$ (Рисунок 1):

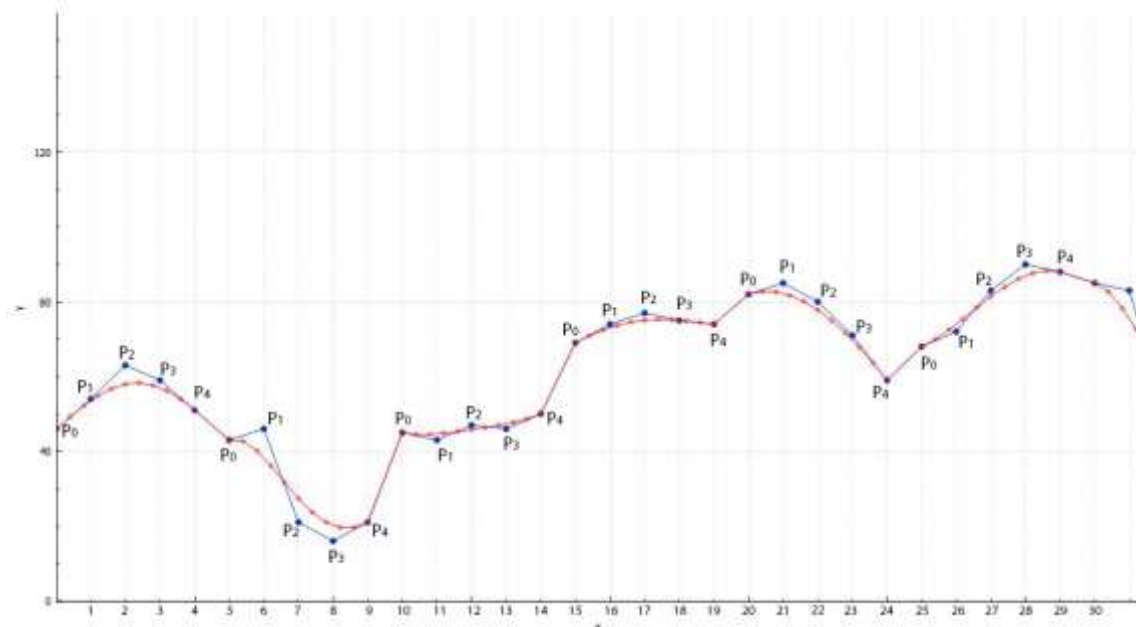


Рисунок 1 – Построение кривой Безье растрового файла с шагом $t=0.1$

По оси Y находятся значения яркостей точек одной из строк изображения S . По Оси X показан порядковый номер точек. Для наглядности в данном примере был взят шаг $t=0.1$. По

графику видно, что на каждые 5 точек яркостей интерполированной картинке (синяя линия), мы имеем 11 точек кривой Безье (красная линия).

Биты информации записываются в P_1 и в P_3 путем взятия такого значения с кривой Безье, у которого младший бит будет равен встраиваемому биту сообщения. При этом, нужно обратить внимание на шаг t , обеспечив достаточный выбор значений R_1 и R_3 для замены P_1 и P_3 . Например, при $t=0.05$ для точки P_1 имеется выбор уже из 9 значений точек кривой Безье, которые можно использовать, округлив их до целого значения, и для точки P_3 аналогично.

В связи с необходимостью округлять полученные значения точек на кривой, возникает проблема возникновения ситуации, когда значения оказываются равными, что сокращает выбор для замены P_1 и P_3 , а также есть вероятность того, что из всех возможных значений множества R_1 или R_3 не окажется ни одного подходящего. Очевидно, проблема будет возникать в изображениях, имеющих однотонные области. Поэтому рекомендуется выбирать более шумные фотографии в качестве контейнера, применяя дополнительно предварительные тесты на пригодность изображения S , а также устанавливать шаг $t=0.01$.

Для того чтобы извлечь встроенное сообщение из контейнера S , необходимо выделить интерполированные значения и получить их младшие биты. Предполагается, что применяемый алгоритм интерполяции заранее известен, так же как и метод встраивания.

Интерполированное изображение размером 450 точек по ширине и 450 точек по высоте позволяет использовать по 112 пересекающихся блоков в каждой строке матрицы пикселей. Таким образом, общее количество блоков для тестовых 8-битных изображений заданного размера составит 50400. Изменяя в каждом блоке по 2 пикселя, мы модифицируем около 50% младших бит изображения. Максимальное количество встроенных бит в изображение размером W по ширине и H по высоте равно:

$$N = 2 \cdot \lfloor W/4 \rfloor \cdot H \quad (4)$$











Таким образом, при правильно подобранных контейнерах с шагом $t=0.01$ максимальная ёмкость встраивания информации методом BCES составит 0.5 бит/пиксель.

Анализ метода BCES

Проанализируем разработанный стеганографический протокол. Для экспериментов возьмем набор из растровых 8-битных изображений размером 225 на 225 в градациях серого, с отсутствием однотонных областей пикселей. После применения интерполяции Лагранжа получим соответствующий набор изображений размером 450 на 450 и встроим случайную последовательность бит методом BCES при $t=0.01$ с заполнением 0.5 бит/пиксель.

Пусть E – это пустой интерполированный контейнер, S – соответствующий заполненный контейнер. Количество встроенных бит 100800. Определим значения разностных показателей визуального искажения [11] для пяти пар контейнеров:

Таблица 1 – Значения разностных показателей искажения

E	S	PSNR	IF	AD
		48.74	0.99	2.04
		48.91	1	1.37
		48.67	1	2.03
		48,99	1	2,79
		48,9	1	2,55

Показатели визуального искажения, использованные в Таблице 1, основаны на анализе пиксельной структуры контейнера и являются наиболее применяемыми в стеганографии изображений. Далее рассмотрим, как вычисляют и интерпретируют данные показатели.

Максимальное соотношение сигнал/шум (PSNR):

$$\text{PSNR} = 10 * \log \frac{255^2}{\varepsilon},$$
 где $\varepsilon = \frac{1}{MN} \sum_{i=0}^M \sum_{j=0}^N (S(i,j) - I(i,j))^2$, M, N – высота и ширина изображения соответственно.

Показатель PSNR часто используется в стеганографии для оценки качества полученных контейнеров [3, 7, 9, 12] и измеряется в зрительных децибелах (Вдб). Здесь ε – это искажение. Чем больше значение PSNR, тем меньше расхождений между сравниваемыми изображениями. Качество обработки изображений считается высоким, если $\text{PSNR} \geq 40$ дБ для 8-битных изображений [13]. Так, в работе [7] рассмотрен метод встраивания на основе интерполяции, имеющий в среднем BPP=1,8 при $\text{PSNR}=35,67$, который является лучшим среди предложенных в работах подобных методов [3-5, 14-16].

Индекс качества изображения (IF):

$$\text{IF} = 1 - \frac{\sum_{x,y} (C_{x,y} - S_{x,y})^2}{\sum_{x,y} (C_{x,y})^2}.$$

Чем ближе данный индекс к 1, тем лучше качество модифицированного изображения по отношению к оригиналу.

Средняя абсолютная разность (AD):

$$\text{AD} = \frac{1}{XY} \cdot \sum_{x,y} |C_{x,y} - S_{x,y}|$$

Низкое значение AD свидетельствует о низком уровне искажений в стегоизображении. Так, предложенный в работе [2] LSB-метод позволил снизить значение AD с 3.45 до 1.85.

Исходя из результатов экспериментов, приведенных в Таблице 1, можно утверждать, что искажения, вносимые стегопреобразованиями по методу BCES являются незначительными и сравнимы с показателями существующих подобных актуальных методов. Существующие стеганографические подходы, основанные на интерполяции, позволяют достигнуть приемлемого уровня PSNR при достаточно высоких показателях BPP. Предложенный в данной статье алгоритм имеет лучшие показатели качества, но уступает в ёмкости встраивания информации в контейнер. Дальнейшее увеличение показателя BPP метода BCES может быть легко достигнуто при использовании методов сжатия сообщений [17]. Таким образом, стegosистема BCES может успешно применяться в области защиты конфиденциальных данных и авторских прав.

Список литературы

1. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. Москва : СОЛОН-ПРЕСС, 2017. – 262 с.
2. Tutuncu, Kemal & çataltaş, Özcan. (2021). Compensation of degradation, security, and capacity of LSB substitution methods by a new proposed hybrid n-LSB approach. Computer Science and Information Systems. 18. 1311-1332. 10.2298/CSIS210227048T.
3. Jung K. H., Yoo K. Y. Data hiding method using image interpolation//Comput Stand Interfaces, 2009. V. 31, iss.2. pp. 465-470.

4. Lee C-F, Huang Y-L. An efficient image interpolation increasing payload in reversible data hiding//Expert Syst Appl. 2012. V. 39, iss.8. pp. 6712-6719.
5. Ahmad A. M., Ali A. H., Mahmoud F. An improved capacity data hiding technique based on image interpolation//Multimed Tools Appl. 2019. V.78, iss.6. pp. 7181-7205.
6. Нагиева А. Ф., Вердиев С. Г. Реверсивный стеганографический метод сокрытия информации, основанный на интерполяции изображений//Компьютерная оптика. 2022. – Т. 46, № 3. С. 465-472.
7. Mahasree M. Improved Reversible Data Hiding in Medical images using Interpolation and Threshold based Embedding Strategy//International Journal of Emerging Trends in Engineering Research. V. 8, 2020. pp. 3495-3501
8. Lu Tzu-Chuen, Huang Shi-Ru, Huang Shu-Wen Reversible hiding method for interpolation images featuring a multilayer center folding strategy//Soft Computing. V. 25, iss.7. 2021. pp.161-180.
9. Евсютин О. О., Кокурина А. С., Мещеряков Р. В. Алгоритмы встраивания информации в цифровые изображения с применением интерполяции//Доклады Томского государственного университета систем управления и радиоэлектроники. 2015. № 4(38). С. 108-112.
10. Bézier, P.E. Numerical Control-Mathematics and applications. London: John Wiley and Sons, 1972. p.240
11. Коханович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. К.: МК-Пресс, 2006, 288 с.
12. Kumar, Neeraj & Kumar, Rajeev & Malik, Aruna & Singh, Samayveer & Jung, Ki-Hyun. (2023). Reversible data hiding with high visual quality using pairwise PVO and PEE. Multimedia Tools and Applications. 82. 1-26. 10.1007/s11042-023-14867-3.
13. Kumari, Lalitha & Ramanathan, Pandian & Rani, J. & Vinothkumar, D. & Sneha, Adeline & Amalarani, V. & S, Bestley. (2017). Selection of optimum compression algorithms based on the characterization on feasibility for medical image. Biomedical Research (India). 28. . pp. 5633-5637.
14. Tang, Mingwei & Hu, Jie & Song, Wen. (2014). A high capacity image steganography using multi-layer embedding. Optik - International Journal for Light and Electron Optics. 125. 3972–3976. 10.1016/j.ijleo.2014.01.149
15. Hu, Jie and Tianrui Li. “Reversible steganography using extended image interpolation technique.” *Comput. Electr. Eng.* 46 (2015): pp.447-455
16. T. Lu. An interpolation-based lossless hiding scheme based on message recoding mechanism, *Optik*, Elsevier, Vol. 130, pp. 1377-1396, 2017
17. Shanmugasundaram S., Lourdusamy R.: A Comparative Study Of Text Compression Algorithms. *International Journal of Wisdom Based Computing*. 1 (2011) pp.68-76.

References

1. Gribunin V. G., Okov I. N., Turintsev I. V. Digital steganography. Moscow : SOLON-PRESS, 2017. – p.262
2. Tutuncu, Kemal & çataltaş, Özcan. (2021). Compensation of degradation, security, and capacity of LSB substitution methods by a new proposed hybrid n-LSB approach. *Computer Science and Information Systems*. 18. 1311-1332. 10.2298/CSIS210227048T.

3. Jung K. H., Yoo K. Y. Data hiding method using image interpolation // *Comput Stand Interfaces*, 2009. V. 31, iss.2. pp. 465-470.
 4. Lee C-F, Huang Y-L. An efficient image interpolation increasing payload in reversible data hiding // *Expert Syst Appl*. 2012. V. 39, iss.8. pp. 6712-6719.
 5. Ahmad A. M., Ali A. H., Mahmoud F. An improved capacity data hiding technique based on image interpolation // *Multimed Tools Appl*. 2019. V.78, iss.6. pp. 7181-7205.
 6. Nagieva A. F., Verdiev S. G. A reversible steganographic method of information concealment based on image interpolation // *Computer Optics*. 2022. – vol. 46, No. 3. pp. 465-472.
 7. Mahasree M. Improved Reversible Data Hiding in Medical images using Interpolation and Threshold based Embedding Strategy // *International Journal of Emerging Trends in Engineering Research*. V. 8, 2020. pp. 3495-3501
 8. Lu Tzu-Chuen, Huang Shi-Ru, Huang Shu-Wen Reversible hiding method for interpolation images featuring a multilayer center folding strategy // *Soft Computing*. V. 25, iss.7. 2021. pp. 161-180.
 9. Evsyutin O. O., Kokurina A. S., Meshcheryakov R. V. Algorithms for embedding information into digital images using interpolation // *Reports of the Tomsk State University of Control Systems and Radioelectronics*. 2015. No. 4(38). pp. 108-112.
 10. Bézier, P.E. *Numerical Control-Mathematics and applications*. London: John Wiley and Sons, pp.1972. 240
 11. Kokhanovich G.F., Puzyrenko A.Yu. *Computer steganography. Theory and practice*. K.: MK-Press, 2006, pp.288
 12. Kumar, Neeraj & Kumar, Rajeev & Malik, Aruna & Singh, Samayveer & Jung, Ki-Hyun. (2023). Reversible data hiding with high visual quality using pairwise PVO and PEE. *Multimedia Tools and Applications*. 82. 1-26. 10.1007/s11042-023-14867-3.
 13. Kumari, Lalitha & Ramanathan, Pandian & Rani, J. & Vinothkumar, D. & Sneha, Adeline & Amalarani, V. & S, Bestley. (2017). Selection of optimum compression algorithms based on the characterization on feasibility for medical image. *Biomedical Research (India)*. 28. pp.5633-5637.
 14. Tang, Mingwei & Hu, Jie & Song, Wen. (2014). A high capacity image steganography using multi-layer embedding. *Optik - International Journal for Light and Electron Optics*. 125. 3972–3976. 10.1016/j.ijleo.2014.01.149
 15. Hu, Jie and Tianrui Li. “Reversible steganography using extended image interpolation technique.” *Comput. Electr. Eng*. 46 (2015): pp. 447-455
 16. T. Lu. An interpolation-based lossless hiding scheme based on message recoding mechanism, *Optik*, Elsevier, Vol. 130, pp. 1377-1396, 2017
 17. Shanmugasundaram S., Lourdusamy R.: A Comparative Study Of Text Compression Algorithms. *International Journal of Wisdom Based Computing*. 1 (2011) pp.68-76.
-