

УДК 004.056.5

О.О. Евсютин, А.С. Кокурина, Р.В. Мещеряков

Алгоритмы встраивания информации в цифровые изображения с применением интерполяции

Представлен обзор основных алгоритмов встраивания информации в цифровые изображения с применением интерполяции, а также предложена собственная модификация одного из данных алгоритмов. Выполнено сравнение рассмотренных алгоритмов по таким характеристикам, как пиковое отношение сигнал/шум и максимальная ёмкость.

Ключевые слова: информационная безопасность, стеганография, цифровые изображения, встраивание информации в пространственную область, интерполяция.

В современном мире обеспечение конфиденциальности информации играет важную роль [1]. Один из подходов к решению данной задачи основан на использовании методов цифровой стеганографии, позволяющих организовывать скрытую передачу секретных информационных последовательностей в цифровых объектах [2, 3].

Данная работа посвящена встраиванию информации в цифровые изображения.

Существует большое количество методов и алгоритмов сокрытия информации в цифровых изображениях. Наиболее распространённым является метод замены наименее значащих битов (LSB), согласно которому для записи сообщения используются младшие один-два бита пикселей цифрового изображения, несущие в себе наименьшее количество информации, воспринимаемой зрением человека [3]. К его преимуществам относятся простота реализации, высокая ёмкость и качество стегоизображения. Также к методам сокрытия информации в пространственной области изображений относятся методы, основанные на матричных преобразованиях блоков пикселей [4, 5], метод «плюс-минус один», при котором значения пикселей увеличиваются или уменьшаются на единицу по некоторому правилу [6], и др.

Однако перечисленные методы в общем случае не обеспечивают возможность восстановления исходного изображения после извлечения встроеного сообщения из стегоконтейнера. Такую возможность позволяют обеспечить методы стеганографического встраивания информации в цифровые изображения, основанные на применении интерполяции.

Интерполяция изображений – это увеличение их размера. Суть интерполяции заключается в использовании имеющихся данных для получения ожидаемых значений в неизвестных точках. Так как интерполяция – это некоторое приближение, то даже при изменении размера одного и того же изображения можно получить разные результаты в зависимости от выбранного алгоритма интерполяции [7].

Идея стеганографических методов, основанных на интерполяции, заключается в том, чтобы встраивать секретную информацию не в само оригинальное изображение, а в изображение-контейнер, полученное путём увеличения оригинала, причём модификации подвергаются только полученные при интерполяции значения пикселей. При извлечении секретных данных также воссоздаётся изображение-контейнер, и используется разница между ним и стегоизображением, что позволяет получить не только спрятанное сообщение, но и восстановленное по неизменённым пикселям оригинальное изображение.

В данной работе представлен обзор основных методов и алгоритмов встраивания информации в цифровые изображения с применением интерполяции, включающий в том числе собственную модификацию одного из данных алгоритмов.

Обзор существующих методов. Все рассматриваемые в статье алгоритмы встраивания информации в цифровые изображения с применением интерполяции работают по одной схеме.

На вход подаётся изображение I размером $M \times N$ и секретное сообщение, представляющее собой двоичную последовательность. Изображение-стегоконтейнер S размером $2M \times 2N$ формируется из исходного изображения с помощью некоторого алгоритма интерполяции.

Перед встраиванием контейнер разбивается на неперекрывающиеся блоки размером 2×2 , в каждом из которых один из пикселей, являющийся пикселем оригинального изображения, принимает-

ся опорным. После этого для каждого из пикселей отдельно взятого блока рассчитывается его отклонение от опорного значения d_k , $k = \overline{1,3}$. Количество битов сообщения n_k , которые могут быть встроены в пиксель, рассчитывается по формуле

$$n_k = \lceil \log_2 |d_k| \rceil. \quad (1)$$

От встраиваемой битовой строки отделяют последовательность из n_k битов и преобразуют её в целочисленное значение b_k .

Встраивание осуществляется по следующей формуле:

$$S(i, j) = C(i, j) \pm b_k, \quad (2)$$

где $S(i, j)$ – значение пикселя стегоизображения, знак в выражении определяется конкретным алгоритмом встраивания.

На вход алгоритма извлечения сообщения подаётся стегоизображение S размером $2M \times 2N$. Из опорных пикселей, которые не использовались для записи встраиваемых битов, формируется исходное изображение I размером $M \times N$. К данному изображению применяется алгоритм интерполяции с целью получения изображения-контейнера C , после чего определяется количество битов, скрытых в пикселях стегоизображения, путём сравнения пустого и заполненного контейнера, и осуществляется извлечение секретного сообщения.

Рассмотрим известные методы и алгоритмы стеганографического встраивания информации в цифровые изображения, соответствующие описанной схеме.

В работе [8] представлен метод сокрытия данных NMI. Интерполяция производится следующим образом: пусть $I(i, j)$ – значение пикселя оригинального изображения, тогда значение пикселя изображения-контейнера $C(i, j)$ будет вычислено по формуле

$$C(i, j) = \begin{cases} I(i, j), & \text{если } i = 2m, j = 2n, \\ (I(i, j-1) + I(i, j+1))/2, & \text{если } i = 2m, j = 2n+1, \\ (I(i-1, j) + I(i+1, j))/2, & \text{если } i = 2m+1, j = 2n, \\ (I(i-1, j-1) + C(i-1, j) + C(i, j-1))/3, & \text{иначе,} \end{cases} \quad (3)$$

где $m = 0, 1, \dots, \frac{M}{2} - 1, n = 0, 1, \dots, \frac{N}{2} - 1$.

Значения пикселей стегоизображения рассчитываются следующим образом. Для каждого из непересекающихся блоков размером 2×2 пикселя требуется найти величину d_k по формуле

$$d_k = C(i, j) - C_d, \quad (4)$$

где C_d – левый верхний пиксель блока, $k = \overline{1,3}$, после чего рассчитывается количество битов n_k , которое может быть встроено в блок и его целочисленное представление b_k , и вычисляются значения соответствующих пикселей стегоизображения.

В работе [9] представлен алгоритм INMI, являющийся модификацией предыдущего. Для получения изображения-контейнера сначала необходимо рассчитать значения центральных пикселей окрестности размером 3×3 изображения-контейнера $C(i^*, j^*)$ по формуле

$$C(i^*, j^*) = \frac{I(i^* - 1, j^* - 1) + I(i^* - 1, j^* + 1) + I(i^* + 1, j^* - 1) + I(i^* + 1, j^* + 1)}{4}, \quad (5)$$

где i^*, j^* – координаты центральных пикселей окрестности размером 3×3 изображения-контейнера.

Затем рассчитать значения остальных пикселей по формуле

$$C(i, j) = \begin{cases} (C(i, j-1) + C(i, j+1) + C(i+1, j))/3, & \text{если } i = i^* - 1, j = j^*, \\ (C(i-1, j) + C(i+1, j) + C(i, j+1))/3, & \text{если } i = i^*, j = j^* - 1, \\ (C(i, j-1) + C(i, j+1) + C(i-1, j))/3, & \text{если } i = 2(M-1), \\ (C(i, j-1) + C(i, j+1) + C(i-1, j))/3, & \text{если } i = 2(N-1). \end{cases} \quad (6)$$

После этого изображение делится на Q непересекающихся равных блоков, количество и порядок обработки которых является дополнительной ключевой информацией. Внутри каждого из блоков отдельно обрабатываются подблоки размером 2×2 пикселя, для каждого из которых считаются величины d_k, n_k, b_k и значения пикселей стегоизображения аналогично предыдущему методу.

В работе [10] представлен метод INP, являющийся модификацией метода NMI. Пиксели изображения-контейнера рассчитываются как

$$C(i, j) = \begin{cases} I(i, j), & \text{если } i = 2m, j = 2n, \\ ((I(i, j-1) + I(i, j+1))/2), & \text{если } i = 2m, j = 2n+1, \\ ((I(i-1, j) + I(i+1, j))/2), & \text{если } i = 2m+1, j = 2n, \\ (C(i-1, j) + C(i, j-1))/2, & \text{иначе,} \end{cases} \quad (7)$$

где $m = 0, 1, \dots, \frac{M}{2} - 1, n = 0, 1, \dots, \frac{N}{2} - 1$.

Для элементов каждого блока 2×2 , исключая крайний левый пиксель, рассчитывается d_k :

$$d_k = M - C(i, j), \quad (8)$$

где M – максимальный крайний элемент блока 3×3 , $k = \overline{1, 3}$.

Далее рассчитываются n_k, b_k и значения пикселей стегоизображения аналогично предыдущему методу.

В работе [11] представлен алгоритм CRS. Для интерполяции сначала требуется найти величины I_{\min} и I_{\max} – минимальное и максимальное значения среди крайних пикселей окрестности 3×3 соответственно. Затем необходимо найти величину AD по формуле

$$AD = \frac{3I_{\min} + I_{\max}}{4}. \quad (9)$$

Значения пикселей изображения-контейнера рассчитываются по формуле

$$C(i, j) = \begin{cases} I(i, j), & \text{если } i = 2m, j = 2n, \\ (AD + (C(i, j-1) + C(i, j+1))/2), & \text{если } i = 2m, j = 2n+1, \\ (AD + (C(i-1, j) + C(i+1, j))/2), & \text{если } i = 2m+1, j = 2n, \\ (C(i, j) + C(i+1, j) + C(i, j+1))/3, & \text{иначе,} \end{cases} \quad (10)$$

где $m = 0, 1, \dots, \frac{M}{2} - 1, n = 0, 1, \dots, \frac{N}{2} - 1$.

Величина d_k для элементов блока 3×3 пикселя, исключая крайний левый пиксель, рассчитывается по формуле

$$d_k = \begin{cases} I_{\max} - C(i, j), & \text{если } C(i, j) < (I_{\min} + I_{\max})/2, \\ C(i, j) - I_{\min}, & \text{иначе,} \end{cases} \quad (11)$$

где $k = \overline{1, 3}$.

Далее вычисляются величины n_k, b_k , значения соответствующих пикселей стегоизображения.

Модификация метода INMI. В данной работе получена модификация метода INMI, основанная на использовании интерполяционного полинома Лагранжа второй степени для получения изображения-контейнера.

Интерполяционная формула Лагранжа имеет следующий вид [12]:

$$L(x) = \sum_{i=0}^n y_i p_i(x), \quad (12)$$

где $p_i(x)$ – многочлен степени n , принимающий значение, равное единице, в узле x_i , равное нулю – в остальных узлах $x_k, k \neq i, k, i = \overline{0, n}$.

В нашем случае изображение, полученное путём добавления дополнительных строк и столбцов пикселей к исходному изображению, рассматривается фрагментами по 5 пикселей, пронумерованных от 0 до 4, как показано на рис. 1.

Известные пиксели (0, 2, 4) будем считать узлами интерполяции. Тогда с помощью интерполяционного полинома Лагранжа второй степени найдём неизвестные значения пикселей (1 и 3). Многочлен Лагранжа для трёх узлов интерполяции имеет вид

$$L(x) = y_0 \frac{(x-x_1) \cdot (x-x_2)}{(x_0-x_1) \cdot (x_0-x_2)} + y_1 \frac{(x-x_0) \cdot (x-x_2)}{(x_1-x_0) \cdot (x_1-x_2)} + y_2 \frac{(x-x_0) \cdot (x-x_1)}{(x_2-x_0) \cdot (x_2-x_1)}. \quad (13)$$

Тогда значения пикселей изображения-контейнера можно рассчитать по формуле

$$C_k = C_0 \frac{(x_k - 2) \cdot (x_k - 4)}{8} + C_2 \frac{x_k (x_k - 4)}{-4} + C_4 \frac{x_k (x_k - 2)}{8}, \tag{14}$$

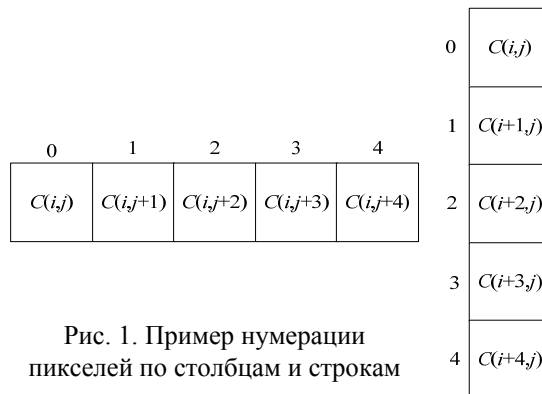
где $k=1, 3$ – номер пикселя во фрагменте из пяти пикселей.

Интерполяция производится сначала по всем строкам, затем – по всем столбцам. Полученное изображение-контейнер может быть использовано для встраивания по методу INMI.

Результаты вычислительных экспериментов. Рассмотренные алгоритмы были протестированы на десяти тестовых изображениях в градациях серого. Исходные изображения размером 512×512 пикселей были уменьшены до размера 256×256 пикселей и в таком виде подавались на вход каждого алгоритма. В процессе встраивания каждое из таких изображений увеличивалось до размера 512×512 пикселей с помощью интерполяции и использовалось для встраивания секретного сообщения.

Для оценки схожести получаемых стегоизображений и исходных изображений размером 512×512 пикселей была использована метрика PSNR (пиковое отношение сигнала к шуму) [3]. В качестве второй оцениваемой характеристики была взята максимальная ёмкость встраивания.

В таблице представлены результаты вычислительных экспериментов для всех рассмотренных алгоритмов. Величина PSNR указана в дБ, ёмкость – бит/пиксель.



Результаты вычислительных экспериментов с рассмотренными алгоритмами

Изображение	NMI		INMI		INP		CRS		Модификация	
	Ёмкость	PSNR	Ёмкость	PSNR	Ёмкость	PSNR	Ёмкость	PSNR	Ёмкость	PSNR
Aerial	1,17	25,24	1,46	24,15	1,88	25,32	2,35	23,59	1,44	24,65
Airplane	0,63	28,94	0,85	27,94	1,25	28,76	1,55	26,99	0,83	28,37
Baboon	1,26	22,57	1,56	22,13	2,04	22,67	2,49	21,58	1,52	22,24
Barbara	0,88	24,42	1,13	23,90	1,51	24,50	1,90	22,98	1,10	24,07
Boat	0,78	27,98	1,06	26,93	1,43	27,89	1,83	25,53	1,04	27,34
Goldhill	0,77	29,72	1,05	28,78	1,45	29,69	1,86	26,19	1,03	29,19
House	0,84	27,52	1,11	26,64	1,45	27,46	1,83	25,15	1,07	27,05
Lena	0,57	31,64	0,80	30,27	1,20	31,61	1,50	27,68	0,78	30,92
Peppers	0,55	30,40	0,77	29,42	1,21	30,18	1,51	27,64	0,76	29,69
Stream	1,21	25,16	1,53	24,35	1,99	24,99	2,47	22,96	1,51	23,89
Сред. значение	0,87	27,36	1,13	26,45	1,54	27,31	1,93	25,03	1,11	26,74

Как видно из представленных в таблице значений, алгоритм NMI лидирует по качеству получаемого стегоизображения, но при этом обеспечивает наименьшую ёмкость встраивания. Наибольшую ёмкость обеспечивает алгоритм CRS, однако при этом значительно страдает качество стегоизображения – у алгоритма CRS оно наименьшее.

Алгоритм INMI продемонстрировал средние результаты. Модификация, предложенная в настоящей статье, улучшает характеристики данного алгоритма: значение PSNR в среднем увеличивается на 0,3 дБ при незначительном уменьшении ёмкости встраивания на 0,02 бит/пиксель.

Лучшее же соотношение ёмкость–качество обеспечивает алгоритм INP. При среднем значении ёмкости 1,54 бит/пиксель алгоритм позволяет получить среднее значение PSNR, равное 27,31 дБ.

Таким образом, сравнение алгоритмов встраивания информации в цифровые изображения с применением интерполяции показало, что, несмотря на сходство рассмотренных алгоритмов, они позволяют получать разные по визуальному качеству и ёмкости стегоизображения.

Заключение. В данной работе был сделан обзор основных алгоритмов встраивания в цифровые изображения с применением интерполяции, включающий также собственную модификацию одного из таких алгоритмов. Результаты применения рассмотренных алгоритмов были сравнены по таким характеристикам, как незаметность встраивания и максимальная ёмкость. На основании полученных результатов был сделан вывод о том, что лучшее соотношение ёмкость–качество обеспечивает метод INP. Одно из возможных направлений дальнейшей работы заключается в получении более эффективных алгоритмических реализаций данного метода [13].

Работа выполнена при поддержке Министерства образования и науки Российской Федерации в рамках мероприятия 1.3 федеральной целевой программы «Исследования и разработки по приори-

тетным направлениям развития научно-технологического комплекса России на 2014–2020 годы» (соглашение о предоставлении субсидии № 14.577.21.0153 от 28 ноября 2014 г.).

Литература

1. Прищеп С.В. Подходы и критерии оценки рисков информационной безопасности / С.В. Прищеп, С.В. Тимченко, А.А. Шелупанов // Безопасность информационных технологий. – 2007. – № 4. – С. 15–21.
2. Гибридная система встраивания интерактивных услуг в цифровой телевизионный поток / С.Ю. Исхаков, А.А. Шелупанов, Р.В. Мещеряков, К.О. Беляков, В.А. Ширшин, А.Л. Шум, В.К. Сарьян // Телекоммуникации. – 2015. – № 1. – С. 11–19.
3. Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: СОЛОН-ПРЕСС, 2009. – 272 с.
4. Chowdhury N. An Efficient Method of Steganography using Matrix Approach / N. Chowdhury, P. Manna // I.J. Intelligent Systems and Applications. – 2012. – Vol. 1. – P. 32–38.
5. Abdullallah W.M. Mix column transform based on irreducible polynomial mathematics for color image steganography: A novel approach / W.M. Abdullallah, A.M.S. Rahma, A.-S.K. Pathan // Computers and Electrical Engineering. – 2014. – Vol. 40. – P. 1390–1404.
6. Zhang W. A Double Layered «Plus-Minus One» Data Embedding Scheme / W. Zhang, X. Zhang, S. Wang // IEEE Signal Processing Letters. – 2007. – Vol. 14, № 11. – P. 848–851.
7. Интерполяция цифрового изображения [Электронный ресурс]. – Режим доступа: <http://www.cambridgeincolour.com/ru/tutorials/image-interpolation.htm>, свободный (дата обращения: 22.09.2015).
8. Jung K.-H. Data hiding method using image interpolation / K.-H. Jung, K.-Y. Yoo // Computer Standards & Interfaces. – 2009. – Vol. 31. – P. 465–470.
9. A Reversible Data Hiding Method Using Improved Neighbor Mean Interpolation and Random-Block Division / L. Liu, T. Chen, S. Zhu, W. Hong, X. Si // Information Technology Journal. – 2014. – Vol. 13, № 15. – P. 2374–2384.
10. Lee C.-F. An efficient image interpolation increasing payload in reversible data hiding / C.-F. Lee, Y.-L. Huang // Expert Systems with Applications. – 2012. – Vol. 39. – P. 6712–6719.
11. Tang M. A high capacity image steganography using multi-layer embedding / M. Tang, J. Hu, W. Song // Optik – International Journal for Light and Electron Optics. – 2014. – Vol. 125, № 15. – P. 3972–3976.
12. Лапчик М.П. Численные методы: учеб. пособие для студ. вузов / М.П. Лапчик, М.И. Рагулина, Е.К. Хеннер. – М.: Изд. центр «Академия», 2004. – 384 с.
13. Встраивание криптографических функций в систему связи с ограниченными ресурсами / С.К. Росошек, Р.В. Мещеряков, А.А. Шелупанов, С.С. Бондарчук // Вопросы защиты информации. – 2004. – № 2. – С. 22–25.

Евсютин Олег Олегович

Канд. техн. наук, доцент каф. безопасности информационных систем (БИС) ТУСУРа

Тел.: 8 (382-2) 70-15-29

Эл. почта: eo0@keva.tusur.ru

Кокурина Анна Сергеевна

Студентка каф. БИС ТУСУРа

Тел.: 8 (382-2) 70-15-29

Эл. почта: annakokurina94@yandex.ru

Мещеряков Роман Валерьевич

Д-р техн. наук, профессор, заведующий каф. БИС, проректор по научной работе и инновациям ТУСУРа

Тел.: 8 (382-2) 70-15-29

Эл. почта: mrv@keva.tusur.ru

Evsutin O.O., Kokurina A.S., Meshcheryakov R.V.

Algorithms for data hiding in digital images using interpolation

This paper proposes review of algorithms for data hiding in digital images using interpolation and modification of one of described algorithms. The comparison of maximum capacity and the peak signal-to-noise ratio between examined algorithms is shown.

Keywords: information security, steganography, digital images, spatial domain data hiding, interpolation.