DOI: 10.55648/1998-6920-2023-17-3-12-22 УДК 003.26

Разработка метода встраивания информации в растровые изображения с помощью интерполяции Лагранжа и кривых Безье *

Е. Ю. Мерзлякова

Сибирский гос. унив. телекоммуникаций и информатики (СибГУТИ)

Аннотация: Статья посвящена актуальному направлению – стеганографии цифровых изображений с использованием интерполяции. Проведен обзор методов встраивания сообщений в растровые файлы, разработан стеганографический метод встраивания в растровые изображения с использованием интерполяции Лагранжа и формулы кривой Безье по пяти точкам. В данной работе подробно рассмотрен протокол разработанной стегосистемы BCES, проанализированы частные случаи и ограничения метода, получен результат RS-анализа, который показал стегоустойчивость метода BSEC.

Ключевые слова: стеганография, цифровые изображения, встраивание информации, интерполяция, стегоанализ.

Для цитирования: Мерзлякова Е. Ю. Разработка метода встраивания информации в растровые изображения с помощью интерполяции Лагранжа и кривых Безье // Вестник СибГУТИ. 2023. Т. 17, № 3. С. 12–22. https://doi.org/10.55648/1998-6920-2023-17-3-12-22.

Статья поступила в редакцию 20.04.2023;
переработанный вариант – 02.05.2023;
принята к публикации 04.05.2023.

1. Введение

Стеганография – это наука об организации передачи секретного сообщения таким образом, чтобы не только содержание сообщения, но и сам факт его передачи были скрыты ото всех незаконных получателей. Такую задачу можно решить, встраивая секретные сообщения в некоторые файлы, называемые контейнерами, чтобы никто, кроме отправителя, не имел доступа одновременно к пустому и заполненному контейнерам. Если недоброжелатель не знает метода встраивания, то стеганографическое сообщение нельзя удалить без значительного искажения контейнера. При этом в совершенной стегосистеме [1] пустые и заполненные контейнеры статистически неразличимы, что делает задачу выявления скрытого сообщения достаточно трудной.

Методы компьютерной стеганографии разделяются по назначению: защита конфиденциальных данных, защита авторских прав, аутентификация данных [2]. В качестве контейнеров могут использоваться различные файлы, не вызывающие подозрения при передаче. Например, аудиофайлы, видеофайлы, различные исполняемые файлы и цифровые фотографии. Стеганография в изображениях представляет собой отдельную область исследований [3].

* Работа выполнена в рамках государственного задания № 071-03-2023-001 от 19.01.2023.

В данной работе в качестве контейнеров рассматриваются цифровые фотографии в растровом формате. Для такого вида контейнеров существует большое количество стеганографических алгоритмов, среди которых распространены методы замены наименее значащих битов (LSB) [4].

Максимальное количество информации, которое можно записать в растровый контейнер при использовании LSB-методов внедрения в черно-белое изображение, составляет 1/8 от размера изображения. LSB-методы имеют множество модификаций и постоянно улучшаются. Так, в работе [5] была предложена схема сокрытия информации в младших битах растрового изображения, использующая кодирование внедряемого сообщения в соответствии с оценками вероятностей появления значений 0 и 1 в младших битах при минимальном искажении статистики, свойственной пустому контейнеру. Затем в [6] предлагалось соединить такую схему с известным методом встраивания LSB ±1 [7]. Способ внедрения сообщения по типу LSB ±1 позволил усовершенствовать исходную схему в плане стойкости к стегоанализу, в то же время использование статистической модели приблизило схему к совершенной. Также к методам сокрытия информации в пространственной области изображений относятся методы, основанные на матричных преобразованиях блоков пикселей [8, 9].

В работе [10] впервые было предложено использовать методы интерполяции для стеганографии изображений в целях повышения качества контейнера. Следуя данной идее, сначала изображение интерполируется, а затем полученный контейнер используется для встраивания данных. В дальнейшем этот способ стал применяться в разработке таких стеганографических методов, как INP [11], NIE [12], реверсивный метод сокрытия информации [13], метод обратимого сокрытия данных в медицинских изображениях [14], метод обратимого сокрытия для интерполяционных изображений с использованием стратегии многослойного сгибания по центру [15] и других.

Обзор основных алгоритмов встраивания информации в цифровые изображения с применением интерполяции, а также модификация одного из данных алгоритмов были предложены в [16], а в [17] был произведен стегоанализ одного из методов, используя RS-стегоанализ [18]. При отсутствии стегоаналитического алгоритма, способного обнаружить факт наличия скрытой информации, стегосистему можно считать стойкой в практическом смысле [19]. Но в отношении исследований в области методов сокрытия данных в изображениях на основе интерполяции для оценки стегосистем в большинстве источников применяются лишь два критерия качества: сравнительный объем встроенной информации (BBP) и пиковое отношение сигнал-шум (PSNR). Более полные результаты исследования методов встраивания можно получить, если проводить эксперименты на больших выборках изображений и применить доступные методы стегоанализа.

Цель настоящей работы состоит в построении и исследовании стегосистемы для растровых изображений с применением интерполяции Лагранжа и кривых Безье. Ожидается получить алгоритм встраивания информации в растровые файлы, расширяющий методы использования интерполяции в стегосистемах, а также имеющий стойкость к стегоанализу RS.

2. Описание стеганографического метода

В данной работе проводимые эксперименты применялись только на 8-битных BMP-файлах в градациях серого из-за простоты их программной обработки, но все полученные результаты автоматически переносятся на случай сохранения изображения в файлах других форматов, использующих неискажающие методы сжатия: tiff, png, pcx, tga, pgm.

В растровом изображении с 8 битами на пиксель каждый байт данных матрицы точек является указателем на 4-байтовое значение RGB — красного (R), зелёного (G) и синего (B) цвета. Яркость каждой составляющей представлена 8-битным числом и может изменяться в диапазоне от 0 до 255. При этом изображение в градациях серого имеет одинаковые значения для составляющих R, G и B точки.

Процесс обработки стеганографического сообщения будет включать следующие объекты:

- сообщение – псевдослучайная двоичная последовательнось;
- контейнер – растровое 8-битное изображение в градациях серого, полученное путем применения интерполяции Лагранжа к цифровой фотографии, размер которой 450 x 450 пикселей;
- стегоконтейнер – контейнер, в который встроено сообщение.

Так как первоначально контейнер был проинтерполирован по алгоритму Лагранжа, и тем самым был увеличен в 2 раза в сравнении с исходной фотографией, то, помимо оригинальных пикселей, в нем присутствуют интерполированные значения. Перед встраиванием контейнер разбивается на блоки размером 1×5, в каждом из которых три значения являются пикселями оригинального изображения. Используя эти значения пикселей, предлагается воспользоваться формулой кривой Безье, чтобы получить плавные переходы от точки к точке. Для этого мы берем пиксели интерполированного изображения группами по 5 точек и строим кривую Безье по формуле:

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

где $n = 4$, $P(t)$ – ордината опорной точки кривой Безье, P_i – значение цвета пикселя изображения, $t \in [0,1]$. Шаг для t может принимать значения 0.1 или меньше. Чем меньше значение шага, тем больше значений кривой мы получаем. Блоки точек пересекаются так, что последняя точка текущего блока является первой точкой следующего блока.

Формулы кривой Безье используются во многих отраслях науки [20–23]. Кривая Безье является частным случаем многочленов Бернштейна, представляет собой параметрическую кривую и определяется следующим выражением:

$$B(t) = \sum_{i=0}^{n} P_i \cdot b_{i,n}(t), \quad 0 \le t \le 1, \tag{2}$$

где n – количество опорных точек;

i – номер опорной точки;

t – шаг;

P – координата опорной точки;

$b(t)$ – базисная функция кривой Безье.

Координаты кривой описываются в зависимости от параметра $t \in [0,1]$:

- для двух точек:
$$P = (1-t)P_1 + t \cdot P_2 \ ;$$
- для трёх точек:
$$P = (1-t)^2 P_1 + 2(1-t)t \cdot P_2 + t^2 \cdot P_3 ;$$
- для четырёх точек:
$$P = (1-t)^3 P_1 + 3(1-t)^2 t \cdot P_2 + 3(1-t)t^2 \cdot P_3 + t^3 \cdot P_4 ;$$
- для пяти точек:
$$P = (1-t)^4 \cdot P_1 + 4 \cdot (1-t)^3 \cdot t \cdot P_2 + 6 \cdot (1-t)^2 \cdot t^2 \cdot P_3 + 4 \cdot (1-t) \cdot t^3 \cdot P_4 + t^4 \cdot P_5 .$$

Далее перейдем к описанию метода встраивания битов сообщения. Назовем предлагаемый алгоритм BCES (Bezier Curves Embedding Strategy). Рассмотрим группу из пяти значений яркости пикселей интерполированного растрового изображения: $(P_0, P_1, P_2, P_3, P_4)$. Точки P_0, P_2, P_4 являются значениями яркостей пикселей оригинального изображения, а значения P_1 и P_3 являются добавленными путем интерполяции. Обозначим значения точек кривой Безье,

вычисленных между P_0 и P_2, множеством $R_1 = \{r_1, \ldots, r_k\}$, а между P_2 и P_4 – множеством $R_3 = \{r_1, \ldots, r_k\}$, где k – это количество значений при данном шаге t. Параметр k фактически представляет собой количество отрезков, на которые делится кривая, проходящая от точки P_0 до точки P_4, за исключением первого и последнего отрезков, а также за исключением тех двух отрезков, которые окружают значение кривой, соответствующей P_2. Таким образом, k вычисляется по следующей формуле:

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

Множество значений из R_1 можно использовать для замены точки P_1, а множество значений из R_3 – соответственно для замены P_3. Краевые значения на кривой, соответствующие P_0, P_2 и P_4, не используются для замены значений P_1 и P_3, так как они соотносятся с теми пикселями изображения, которые изначально составляли матрицу пикселей до процесса интерполяции. Встраивание бита информации m в точку P_1 происходит по следующему алгоритму:

ВХОД: Значение яркости: P_1; бит сообщения: m; значения точек кривой Безье, вычисленных между P_0 и P_2: $R_1 = \{r_1, \ldots, r_k\}$.

ВЫХОД: Значение яркости P_1, содержащее бит сообщения m.

1. IF $LSB(P_1) \neq m$ THEN
2. FOR i=1, 2,…, k DO
3. IF $LSB(r_i) = m$ THEN $P_1 \leftarrow \lfloor r_i \rfloor$.
4. RETURN P_1.

Аналогично происходит встраивание бита информации m в точку P_3, используя R_3.

Чтобы данный алгоритм работал, необходимо задать такой шаг t, который обеспечит достаточный выбор значений R_1 и R_3 для замены P_1 и P_3.

Рассмотрим график усредненных яркостей пикселей и построенной кривой Безье по их значениям с шагом t = 0.05 (рис. 1):

По оси Y синим цветом показан график переходов значений яркостей точек изображения, взятых из первой строки матрицы пикселей по порядку, а красным цветом показана кривая Безье. По оси X идет порядковый номер точек.

При t = 0.05 для точки P_1 имеется выбор из 9 значений точек кривой Безье, которые можно использовать, округлив их до целого значения, и для точки P_3 также имеется выбор из 9 значений. После замены значений P_1 и P_3 строится отрезок кривой Безье по следующим пяти точкам пикселей, причем P_5 является P_1 для следующего подряд блока.

Алгоритм извлечения встроенных бит довольно прост, так как в каждом втором значении яркостей пикселей изображения содержится искомый бит.

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. При встраивании в каждый блок по 2 бита максимальное количество встроенных бит в изображение размером W по ширине и H по высоте равно:

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

Для изображений, используемых в рамках данной работы, N = 100800 бит, то есть примерно 12.3 Кбайт.

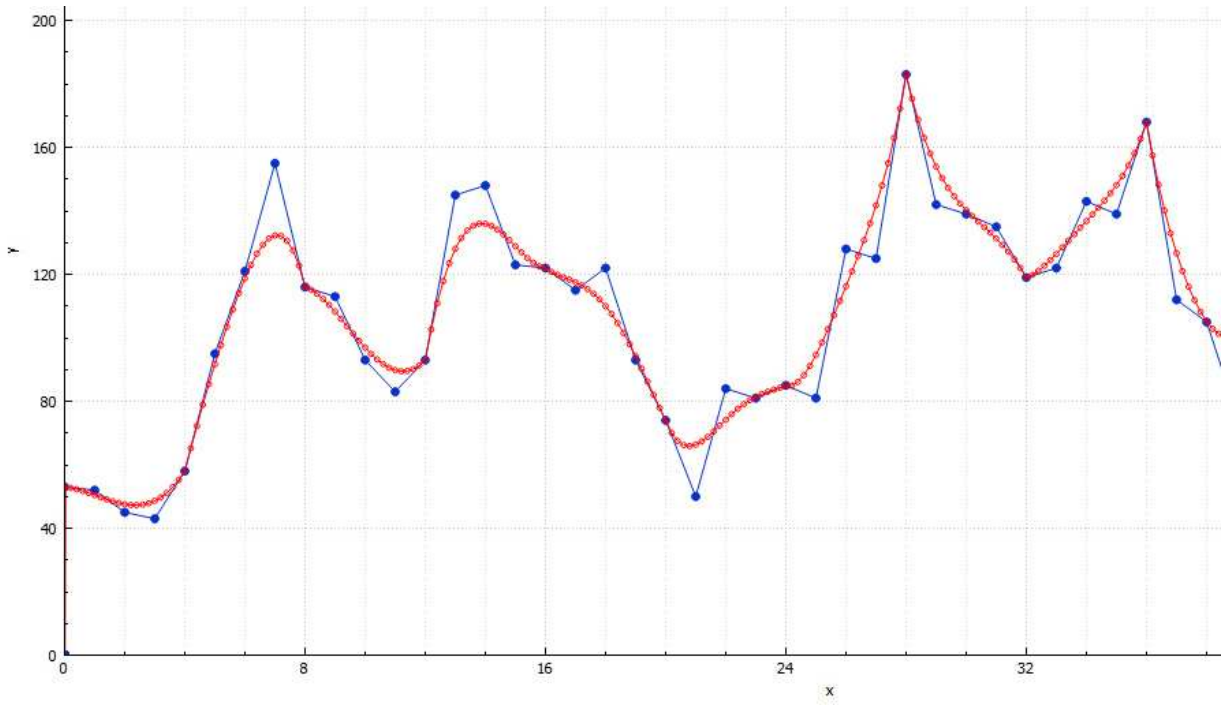

Рис. 1. Построение кривой Безье для файла 005.bmp с шагом $t = 0.05$

3. Ограничения метода BSEC

При реализации рассмотренного алгоритма встраивания возникает следующее ограничение. Так как значения точек кривой Безье должны быть округлены до целого, то мы можем получать одинаковые значения, которые сократят выбор для замены P_1 и P_3. Может возникнуть ситуация, когда из всех возможных значений множества r не окажется ни одного подходящего. Более вероятно, проблема будет возникать в изображениях, имеющих однотонные области. Эксперимент на наборе из 10 контейнеров показал, что в среднем не удастся записать бит сообщения в 293 точки (0.3 %) (табл. 1).

Таблица 1. Количество проблемных точек в контейнерах при $t = 0.05$

Стегоконтейнер, $N = 100800$	Количество неудачных точек	Неудачные точки, %
1.bmp	209	0.2
2.bmp	345	0.3
3.bmp	288	0.3
4.bmp	177	0.2
5.bmp	226	0.2
6.bmp	973	1
7.bmp	240	0.2
8.bmp	246	0.2
9.bmp	193	0.2
10.bmp	223	0.2
Среднее значение	293	0.3

Следует отметить, что тестовые изображения являлись довольно шумными фотографиями природы. Контейнер 4.bmp (рис. 2) из представленного набора имел наименьшее количество непригодных точек для встраивания, а контейнер 6.bmp (рис. 3) – наибольшее их количество.

Рис. 2. Контейнер 4.bmp

Рис. 3. Контейнер 6.bmp

Таким образом, на этапе отбора контейнеров для встраивания рекомендуется выбирать такие фотографии, на которых монотонные области отсутствуют. Также для минимизации количества непригодных бит можно установить более короткий шаг *t*.

Рассмотрим подробнее, как значение шага *t* влияет на результат работы метода BCES. Обозначим множество подходящих значений r_i для встраивания каждого очередного бита из $M = \{m_1, \ldots, m_N\}$ как $S_1 = \{s_1, \ldots, s_{k-e}\}$ и $S_3 = \{s_1, \ldots, s_{k-f}\}$, то есть S_1 содержит значения из R_1, а S_3 содержит значения из R_3, такие что их самый младший бит совпадает с текущим битом встраиваемого сообщения. Значения *e* и *f* переменны и зависят от пикселей используемого изображения. Чем меньше шаг *t*, тем меньше вероятность того, что *k* окажется равным *e* или *f*. При возникновении такой ситуации, что $k = e$ либо $k = f$, ни одно из значений множества R_1 либо R_3 не подойдет для встраивания очередного бита сообщения. Если при декодировании не определить наличие такого случая, то возникнет потеря бита сообщения.

Если взять шаг $t = 0.01$, то вероятность возникновения проблемы снизится, так как при $k = 49$ будут получены более объемные S_1 и S_3. Но каким бы маленьким ни был шаг *t*,

количество значений множеств R_1 и R_3 всегда будет ограничено, так как они являются округленными значениями, и даже при максимально возможном количестве построенных точек кривой Безье мы теоретически можем получать равные значения. Поэтому здесь стоит подумать над качеством исходных контейнеров. В табл. 2 приведены результаты аналогичного табл. 1 эксперимента, но при $t = 0.01$.

Таблица 2. Количество проблемных точек в контейнерах при $t = 0.01$

Стегоконтейнер, $N = 100800$	Количество неудачных точек
1.bmp	0
2.bmp	0
3.bmp	0
4.bmp	0
5.bmp	0
6.bmp	885
7.bmp	0
8.bmp	0
9.bmp	0
10.bmp	0
Среднее значение	88.5

Таким образом, установка шага $t = 0.01$ позволила полностью использовать 9 из 10 контейнеров, получая безошибочное декодирование. Непригодный контейнер 6.bmp, представленный на рис. 2, имеет большую однотонную область, заметную невооруженным глазом. Исключив подобные контейнеры, можно использовать метод BCES успешно при максимальном заполнении 0.5 бит/пиксель (BBP).

4. Экспериментальный анализ скрытности

В результате разработан стеганографический протокол, который позволяет встраивать сообщения в растровые файлы с BPP = 0.5. Визуально пустые и заполненные контейнеры не отличаются (рис. 4).

Рис. 4. Пустой контейнер (слева) и заполненный (справа)

Помимо количественных оценок объема внедрения, необходимо определить устойчивость метода BCES к стегоанализу. Стеганостойкость – это процентное соотношение числа цифровых файлов, в которых удалось обнаружить факт наличия встроенных сообщений к общему числу исследуемых файлов [4]. В качестве средства стегоанализа был использован метод RS [18]. RS-анализ использует чувствительный метод двойной статистики, полученной из пространственных корреляций в изображениях. Выходным значением RS-анализа является предполагаемая длина сообщения в исследуемом изображении. Затем это значение может быть сравнено с некоторым пороговым значением для получения маркировки классификатором. Этот метод показывает достаточно точный результат даже на шумных изображениях.

Для того чтобы рассчитать стеганостойкость метода BCES, был сформирован подходящий набор (с отсутствием однотонных областей пикселей) из 100 растровых 8-битных изображений размером 450 на 450 в градациях серого, для которых ошибка первого рода [19] составляла 0 %. Затем контейнеры были заполнены методом BCES при $t = 0.01$, BPP = 0.5.

В табл. 3 приведен результат RS-анализа метода BCES. Длина L предполагаемого сообщения, обнаруженного при помощи RS-анализа, классифицируется как положительная при значении не менее 5 %.

Таблица 3. RS-анализ на наборе заполненных контейнеров (100 картинок)

L	0 %	1–4 %	5 % и более
Доля файлов, %	38	62	0

Таким образом, экспериментально была определена стеганостойкость разработанного метода BCES к обнаружению факта передачи сообщения методом RS. Разработанный метод оказался устойчивым к RS-анализу.

5. Заключение

Итогом данной работы является стеганографическая система BCES встраивания информации в цифровые изображения в градациях серого. При формировании подходящего набора контейнеров ёмкость встраивания постоянна и составляет 0.5 BPP. Разработанный метод был исследован с помощью RS-анализа и показал хорошую стегоустойчивость.

Чтобы повысить уровень защиты информации в методе BCES, достаточно при встраивании и извлечении подбирать такую точку кривой Безье, у которой совпадающий с битом сообщения бит является не самым младшим, а, например, третьим и даже самым старшим, что никак не повлияет на качество метода. Таким образом, стегосистема BCES может применяться в целях защиты конфиденциальных данных и авторских прав.

В дальнейшем планируется реализовать и применить другие алгоритмы стегоанализа для исследования стеганографических методов, использующих интерполяцию цифровых изображений, что позволит провести сравнение разработанного метода с современными стегосистемами.

Литература

1. *Cachin C.* An information-theoretic model of steganography // Lecture Notes in Computer Science (Proc. 2nd Information Hiding Workshop). Springer Verlag. 1998. V. 1525. P. 306–318.
2. *Коханович Г. Ф., Пузыренко А. Ю.* Компьютерная стеганография. Теория и практика. К.: МК-Пресс, 2006. 288 с.
3. *Сейеди С. А., Садыхов Р. Х.* Сравнение методов стеганографии в изображениях // Информатика. 2012. № 1. С. 66–75.

4. *Грибунин В. Г., Оков И. Н., Туринцев И. В.* Цифровая стеганография. Москва : СОЛОН-ПРЕСС, 2017. 262 с.
5. *Елтышева Е. Ю., Фионов А. Н.* Построение стегосистемы на базе растровых изображений с учетом статистики младших бит // Вестник СибГУТИ. 2009. № 1. С. 67–84.
6. *Елтышева Е. Ю.* Построение стегосистемы для растровых изображений на основе стохастической модуляции с учетом статистики младших бит // Вестник СибГУТИ. 2011. № 2. С. 63–75.
7. *Goljan M.* Digital Image Steganography Using Stochastic Modulation // Proc. SPIE, Electronic Imaging, Security, Steganography and Watermarking of Multimedia Contents, Santa Clara, California, 2003. V. 5020. P. 191–202.
8. *Chowdhury N., Manna P.* An Efficient Method of Steganography using Matrix Approach // I. J. Intelligent Systems and Applications. 2012. V. 1. P. 32–38.
9. *Abduallah W. M., Rahma A. M. S., Pathan A.-S. K.* Mix column transform based on irreducible polynomial mathematics for color image steganography: A novel approach // Computers and Electrical Engineering. 2014. V. 40. P. 1390–1404.
10. *Jung K. H., Yoo K. Y.* Data hiding method using image interpolation // Comput. Stand. Interfaces. 2009. V. 31, Is. 2. P. 465–470.
11. *Lee C.-F., Huang Y.-L.* An efficient image interpolation increasing payload in reversible data hiding // Expert Syst. Appl. 2012. V. 39, Is. 8. P. 6712–6719.
12. *Ahmad A. M., Ali A. H., Mahmoud F.* An improved capacity data hiding technique based on image interpolation // Multimed. Tools Appl. 2019. V. 78, Is. 6. P. 7181–7205.
13. *Нагиева А. Ф., Вердиев С. Г.* Реверсивный стеганографический метод сокрытия информации, основанный на интерполяции изображений // Компьютерная оптика. 2022. Т. 46, № 3. С. 465–472.
14. *Mahasree M.* Improved Reversible Data Hiding in Medical images using Interpolation and Threshold based Embedding Strategy // International Journal of Emerging Trends in Engineering Research. 2020. V. 8. P. 3495–3501.
15. *Lu Tzu-Chuen, Huang Shi-Ru, Huang Shu-Wen.* Reversible hiding method for interpolation images featuring a multilayer center folding strategy // Soft Computing. 2021. V. 25, Is. 7. P. 161–180.
16. *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.
17. *Daiyrbayeva E., Yerimbetova A., Nechta I., Merzlyakova E., Toigozhinova A., Turganbayev A.* A Study of the Information Embedding Method into Raster Image Based on Interpolation // Journal of Imaging. 2022. V. 8, № 10. P. 288.
18. *Fridrich J., Goljan M., Du R.* Reliable Detection of LSB Steganography in Grayscale and Color Images // Special Session on Multimedia Security and Watermarking. Ottawa, Canada. 2001. P. 27–30.
19. *Грибунин В. Г., Костюков В. Е., Мартынов А. П., Николаев Д. Б., Фомченко В. Н.* Прикладная стеганография: для студентов, аспирантов, научных работников, изучающих вопросы обеспечения безопасности информации. Саров: Российский Федеральный ядерный центр – Всероссийский научно-исследовательский институт экспериментальной физики, 2021. 484 с.
20. *Bézier P. E.* Numerical Control-Mathematics and applications. London: John Wiley and Sons, 1972. 240 p.
21. *Ntoko N.-M.* A formulation for Bézier-type curves // Computers in Industry. 1990. V. 15, Is. 4. P. 363–368.
22. *Kajla A., Acar T.* Bézier–Bernstein–Durrmeyer type operators // Revista de la Real Academia de Ciencias Exactas, Fisicas y Naturales – Serie A: Matematicas. 2019. V. 114, № 1. P. 1–11.

23. *Wu Y., Li Xin.* Curve intersection based on cubic hybrid clipping // Visual Computing for Industry, Biomedicine and Art. 2022. V. 5, Is.1, № 17. P. 1–13.

Мерзлякова Екатерина Юрьевна
к.т.н., доцент кафедры прикладной математики и кибернетики, Сибирский государственный университет телекоммуникаций и информатики (СибГУТИ, 630102, Новосибирск, ул. Кирова, д. 86), тел. +7 383 2698 272, e-mail: katerina.artist@yandex.ru, ORCID ID: 0000-0001-6847-5588.

Автор прочитал и одобрил окончательный вариант рукописи.
Автор заявляет об отсутствии конфликта интересов.

Development of the method for embedding information into raster images using Lagrange interpolation and Bezier curves

Ekaterina Y. Merzlyakova

Siberian State University of Telecommunications and Information Science (SibSUTIS)

Abstract: The article is devoted to the actual direction – steganography of digital images using interpolation. The review of embedding messages methods in raster files is carried out, the steganographic method of embedding in bitmap images using Lagrange interpolation and the Bezier curve formula for five points is developed. In this paper, the protocol of the developed BCES stegosystem is considered in detail, special cases and limitations of the method are analyzed, the result of RS analysis is obtained showing the stability of the BSEC method.

Keywords: steganography, digital images, information embedding, interpolation, steganalysis.

For citation: Merzlyakova E. Y. Development of the method for embedding information into raster images using Lagrange interpolation and Bezier curves. (in Russian). *Vestnik SibGUTI*, 2023, vol. 17, no. 3, pp. 12-22. https://doi.org/10.55648/1998-6920-2023-17-3-12-22.

The article was submitted: 20.04.2023;
revised version: 02.05.2023;
accepted for publication 05.05.2023.

References

1. Cachin C. An information-theoretic model of steganography. *Lecture Notes in Computer Science (Proc. 2nd Information Hiding Workshop)*. Springer Verlag, 1998, vol. 1525, pp. 306-318.
2. Kohanovich G.F., Puzyrenko A.Ju. *Komp'juternaja steganografija. Teorija i praktika* [Computer steganography. Theory and practice]. K., MK-Press, 2006. 288 p.
3. Sejedi S. A., Sadyhov R. H. Sravnenie metodov steganografii v izobrazhenijah [Comparison of steganography methods in images]. *Informatika*, 2012, no.1, pp. 66–75.
4. Gribunin V. G., Okov I. N., Turincev I. V. *Cifrovaja steganografija* [Digital steganography]. Moscow, SOLON-PRESS, 2017. 262 p.
5. Eltysheva E. Ju., Fionov A. N. Postroenie stegosistemy na baze rastrovyh izobrazhenij s uchetom statistiki mladshih bit [Building a stegosystem based on bitmap images, taking into account the statistics of the lower bits]. *Vestnik SibGUTI*, 2009, no 1, pp. 67-84.

6. Eltysheva E. Ju., Postroenie stegosistemy dlja rastrovyh izobrazhenij na osnove stohasticheskoj moduljacii s uchetom statistiki mladshih bit [Construction of the stegosystem for bitmap images based on stochastic modulation taking into account the statistics of the lower bits]. *Vestnik SibGUTI*, 2011, no 2, pp. 63-75.
7. Goljan M. Digital Image Steganography Using Stochastic Modulation. *Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents*, vol. 5020, Santa Clara, California, 2003, pp. 191-202.
8. Chowdhury N., Manna P. An Efficient Method of Steganography using Matrix Approach. *I.J. Intelligent Systems and Applications*, 2012, vol. 1, pp. 32–38.
9. Abduallah W. M., Rahma A. M. S., Pathan A.-S. K. Mix column transform based on irreducible polynomial mathematics for color image steganography: A novel approach. *Computers and Electrical Engineering*, 2014, vol. 40, pp. 1390–1404.
10. Jung K. H., Yoo K. Y. Data hiding method using image interpolation. *Comput Stand Interfaces*, 2009, no. 31, iss.2, pp. 465-470.
11. Lee C-F, Huang Y-L. An efficient image interpolation increasing payload in reversible data hiding. *Expert Syst Appl*, 2012, no. 39(8), pp. 6712-6719.
12. Ahmad A. M., Ali A. H., Mahmoud F. An improved capacity data hiding technique based on image interpolation. *Multimed Tools Appl*, 2019, no. 78(6), pp. 7181-7205.
13. Nagieva A. F., Verdiev S. G. Reversivnyj steganograficheskij metod sokrytija informacii, osnovannyj na interpoljacii izobrazhenij [Reversible steganographic method of information concealment based on image interpolation]. *Komp'juternaja optika*, 2022, vol. 46, no. 3, pp. 465-472.
14. Mahasree M. Improved Reversible Data Hiding in Medical images using Interpolation and Threshold based Embedding Strategy. *International Journal of Emerging Trends in Engineering Research*, vol. 8, 2020, pp. 3495-3501
15. Lu Tzu-Chuen, Huang Shi-Ru, Huang Shu-Wen Reversible hiding method for interpolation images featuring a multilayer center folding strategy. *Soft Computing*, vol. 25(7), 2021, pp. 161-180.
16. Evsjutin O. O., Kokurina A. S., Meshherjakov R. V. Algoritmy vstraivanija informacii v cifrovye izobrazhenija s primeneniem interpoljacii [Algorithms for embedding information into digital images using interpolation]. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravlenija i radiojelektroniki*, 2015, no. 4(38), pp. 108-112.
17. Daiyrbayeva E., Yerimbetova A., Nechta I., Merzlyakova E., Toigozhinova A., Turganbayev A. A Study of the Information Embedding Method into Raster Image Based on Interpolation. *Journal of Imaging*, vol. 8(10), 2022, p. 288.
18. Fridrich J., Goljan M., Du R. Reliable Detection of LSB Steganography in Grayscale and Color Images. *Special Session on Multimedia Security and Watermarking*, Ottawa, Canada, 2001, pp. 27-30.
19. Gribunin V. G., Kostjukov V. E., Martynov A. P., Nikolaev D. B., Fomchenko V. N. *Prikladnaja steganografija: dlja studentov, aspirantov, nauchnyh rabotnikov, izuchajushhih voprosy obespechenija bezopasnosti informacii.* [Applied steganography: for students, postgraduates, researchers studying information security issues]. Sarov, Rossijskij Federal'nyj jadernyj centr, Vserossijskij nauchno-issledovatel'skij institut jeksperimental'noj fiziki, 2021. 484 p.
20. Bézier P.E. *Numerical Control-Mathematics and applications*. London, J. Wiley and Sons, 1972. 240 p.
21. Ntoko N.-M. A formulation for Bézier-type curves, *Computers in Industry*, 1990, vol. 15, iss. 4, pp. 363-368.
22. Kajla A., Acar T. Bézier–Bernstein–Durrmeyer type operators // *Revista de la Real Academia de Ciencias Exactas, Fisicas y Naturales*, Serie A: Matematicas, 2019, vol. 114, no. 1, pp. 1-11.
23. Wu Y., Li Xin. Curve intersection based on cubic hybrid clipping // *Visual Computing for Industry*, Biomedicine, and Art, 2022, vol. 5, iss.1, no. 17, pp. 1-13.

Ekaterina Y. Merzlyakova

PhD (Engineering), Docent; Docent of the Department of Applied Mathematics and Cybernetics, Siberian State University of Telecommunications and Information Science (SibSUTIS, Russia, 630102, Novosibirsk, Kirov St. 86), phone: +7 383 2698 272, e-mail: katerina.artist@yandex.ru, ORCID ID: 0000-0001-6847-5588.