УДК 003.26

Е.Ю. Елтышева, А.Н. Фионов

ПОСТРОЕНИЕ СТЕГОСИСТЕМ ДЛЯ РАСТРОВЫХ ИЗОБРАЖЕНИЙ МЕТОДОМ ПЕРЕСТАНОВОК

Предлагается метод сокрытия информации в пикселях растрового изображения, записанного в файлах формата BMP, PNG и др., использующих неискажающие методы сжатия. В отличие от известных аналогов, предлагаемый метод внедряет сообщение в растр путем незначительных перестановок соседних байтов яркостей. Проводится RS-анализ разработанного алгоритма и сравнение его с известными аналогами.

Стеганография; стегоанализ; LSB-методы; статистическая модель; арифметическое кодирование; идеальные стегосистемы.

E.Yu. Eltysheva, A.N. Fionov

STEGOSYSTEM CONSTRUCTION FOR THE RASTER IMAGES BY THE PERMUTATION METHOD

A method of data hiding in pixels of raster images, represented as files in BMP, PNG and other formats which employ lossless data compression. In contrast to known analogs, the suggested method embeds data to raster by unimportant permutations of adjacent bytes. RS analysis of the algorithm developed is carried out. An advantage of the suggested method over known analogs is demonstrated.

Steganography; steganalysis; LSB-methods; statistical model; arithmetic coding; ideal stegosystems.

Введение. Цель стеганографии состоит в организации передачи секретных данных так, чтобы сам факт передачи был скрыт ото всех незаконных получателей. В [1] впервые предложена совершенная стегосистема, в которой сообщения, несущие и не несущие скрытую информацию, статистически неразличимы. Основная идея, использованная при построении такой стегосистемы, применяется и в нашем случае, но уже не для вероятностных источников, а для изображений.

В результате проведённых исследований был построен алгоритм внедрения скрытых сообщений в изображения. Мы использовали RS-анализ [2], как один из наиболее эффективных методов выявления скрытой информации. Анализ был проведён на случайной выборке из 800 изображений, и показал, что при уровне заполнения контейнера около 30 % предложенный алгоритм позволяет скрыть наличие встроенного сообщения в 100 % файлов. Для общедоступных стегопрограмм HIDE4PGP и STEGOTOOLS при том же уровне заполнения 30 % RS-анализ наоборот обнаружил наличие встроенной информации практически во всех файлах. Вместе с тем, данный метод имеет достаточно высокую емкость $\log n!/n$ бит на пиксель. Декодирование встроенной информации происходит за счет установленного порядка следования, который можно задать изначально в качестве секретного ключа. Не изменяя фактических значений бит, мы гарантируем безошибочное извлечение информации.

В качестве стегоконтейнера мы будем рассматривать изображения, представляющие собой матрицу пикселей P размером $h \times w$. Для простоты описания условимся под элементом матрицы P понимать только одну обобщённую цветовую составляющую, определяющую действия над всеми тремя.

Метод перестановок основывается на свойстве близко идущих пикселей, которые в типичных изображениях почти одинаковы. Мы разделим тестовый набор файлов на два типа. Первый тип A – это *естественный* тип фотографий, к кото-

рым относятся фотографии с плавным переходом яркостей, преимущественно природных объектов. Второй тип B – это *искусственный* тип фотографий, к которым относятся контрастные фотографии преимущественно искусственных объектов. В экспериментальных исследованиях мы будем использовать два набора тестовых файлов из 400 изображений каждый – *набор A* и *набор B*.

При RS-анализе программа выдает количество встроенной информации (L) в процентах от эмпирической емкости контейнера, которая высчитывается как при LSB-встраивании:

$$C_{\text{LSB}} = 3wh \text{ бит.} \quad (1)$$

Формула (1) означает, что в каждый байт пикселя встраивается 1 бит информации. По значению L можно судить о том, заполнен был контейнер или пуст. Например, в работе [3] установлено, что при $L \geq 5$ % RS-анализ классифицирует контейнер как заполненный. В применении RS-анализа мы будем опираться на эти сведения. В цифровой стеганографии существует два рода ошибок [4]. Предположим, что имеются две гипотезы: H_C и H_S. Если справедлива гипотеза H_C, то контейнер является пустым, а если справедлива H_S, то контейнер содержит сообщение. Правило решения заключается в разбиении множества наблюдений на две части так, чтобы сопоставить одну из двух гипотез каждому контейнеру. В этой задаче различения возможны два типа ошибок: *ошибка первого рода*, которая заключается в установлении гипотезы H_S, когда верной является H_C и *ошибка второго рода*, когда принято решение H_C при верной гипотезе H_S. Например, если при анализе пустого контейнера было принято решение, что он является заполненным, то это означает наличие ошибки первого рода. А если при анализе заполненного контейнера было принято решение, что он пустой, то имеет место ошибка второго рода.

Метод перестановок. Будем рассматривать матрицу P группами из n элементов. Известно, что число всех возможных перестановок равно

$$P_n = n!. \quad (2)$$

Идея заключается в том, что каждой из $n!$ комбинаций мы можем сопоставить кодовый символ. Другими словами, мы имеем дело с задачей нумерации перестановок. Чтобы обеспечить безошибочное декодирование, перестановки необходимо генерировать в лексикографическом порядке, то есть самая первая комбинация всегда будет являться упорядоченной последовательностью. Заметим, однако, что в группе из n элементов вполне возможны повторения. Число всех возможных перестановок с повторениями

$$P(n_1, n_2, \dots, n_k) = \frac{n!}{n_1! \cdot n_2! \dots n_k!}, \quad (3)$$

где $n_1 + n_2 + \cdots + n_k = n$; n_k – количество вхождений k-го элемента.

Итак, первым условием для данного метода будет следующее:

$$P(n_1, n_2, \dots, n_k) > 1,$$

$$P(n_1, n_2, \dots, n_k) > 1. \quad (4)$$

Это значит, что группа, в которой не выполняется условие (4), остается без изменений в файле. При декодировании такие группы просто пропускаются.

Второе условие для каждой группы пикселей будет накладывать ограничения на искажения при встраивании информации:

$$|P_i - P_j| \geq d \text{ для всех } i, j = 1 \dots n \ (i \neq j), \quad (5)$$

где d – установленный порог искажений, значение которого было получено экспериментально на основе низкоуровневых свойств человеческого зрения [4]. Условие (5) обеспечивает отсутствие визуальных искажений при использовании метода перестановок при заданном пороговом значении $d = 3$.

Далее, если группа удовлетворяет условиям (4) и (5), то для нее формируется алфавит кодовых символов $A = \{1 \dots m\}$, где $m = P(n_1, n_2, \dots, n_k)$, т.е. каждый кодовый символ сопоставлен с определенной комбинацией группы. Комбинации генерируются строго в лексикографическом порядке и кодовый символ «1» всегда соответствует группе, упорядоченной в прямом порядке. Затем сформированный алфавит поступает на вход арифметического декодера. Все символы алфавита являются равновероятными для каждой группы. Арифметическому декодеру указывается это распределение вероятностей, в соответствии с которым он и декодирует этот символ, рассматривая зашифрованное сообщение как код, построенный ранее соответствующим арифметическим кодером. Полученный символ на выходе арифметического декодера определяет номер перестановки для текущей группы. Чтобы восстановить зашифрованное сообщение из его кода, требуется, наоборот, применить арифметический кодер, которому указываются те же самые распределения вероятностей, что и декодеру. Таким образом, арифметическому кодеру подается на вход соответственный номер перестановки очередной группы, удовлетворяющей условиям (4) и (5), в результате чего на выходе мы получаем декодированное сообщение. Наглядная схема данного метода приведена на рис. 1.

Для повышения стойкости метода необходимо менять лексикографический порядок следования байт в группе на каждом шаге в соответствии с секретной псевдослучайной битовой последовательностью, полученной с помощью того же шифра, которым шифруется встраиваемое сообщение. Биты последовательности используются для определения порядка. Следовательно, злоумышленник, располагая сведениями о методе, но, не зная секретной информации, не сможет выделить из контейнера ту часть, которая является зашифрованным сообщением.

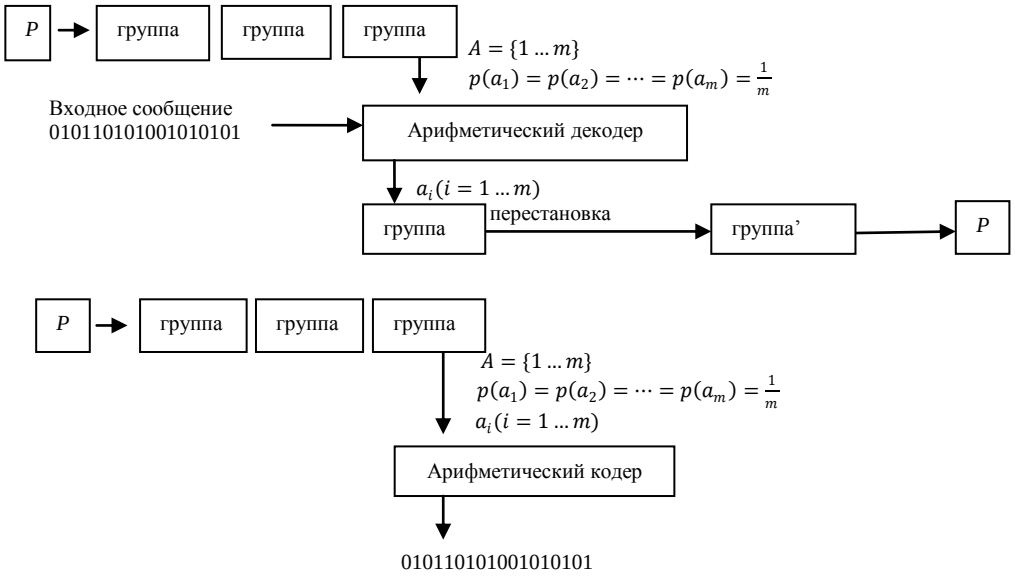

Рис. 1. Схемы кодирования и декодирования

Остановимся подробней на том, каким образом происходит разбиение матрицы P на группы. Количество групп в матрице определяется по формуле:

$$K_g = \frac{3 \cdot w \cdot h}{n}, \quad (6)$$

где w – количество столбцов в матрице, h – количество строк в матрице, n – длина группы. В каждую группу мы можем встроить максимум $\log n!$ бит. Ясно, что чем больше размер группы, тем выше емкость контейнера. Эмпирическая емкость метода определяется на основе (1) и (6) следующим образом:

$$C_n = K_g \cdot \log n! = \frac{C}{n} \cdot \log n!. \quad (7)$$

Заметим, что это максимальное значение количества информации, которое можно встроить при допущении, что каждая группа удовлетворяет условиям (4) и (5), а также не имеет повторяющихся элементов. На практике такой случай возможно получить только если создать контейнер искусственно. В обычных же контейнерах с возрастанием размера группы увеличивается и вероятность того, что такая группа не будет удовлетворять условиям (4) и (5) и будет содержать повторяющиеся элементы, что существенно уменьшит фактическую емкость. Поэтому нам необходимо экспериментально определить оптимальный размер группы. В качестве зашифрованного сообщения возьмем случайные данные. Процент заполнения каждого контейнера определяется в соответствии с общей эмпирической емкостью C_{LSB}, средние значения приводятся в табл. 1 при установленном пороге искажений $d = 3$.

Таблица 1

Средний процент заполнения контейнеров

n	Схема формирования группы	Тестовый набор A	Тестовый набор B
3	Линейно, из идущих подряд пикселей	28%	34%
4	Линейно, из идущих подряд пикселей	27%	34%
3	В форме треугольников	18%	20%
4	В форме квадратов 2x2	23%	32%

По результатам, приведенным в табл. 1, можно прийти к выводу, что увеличение размера группы не приведет к лучшим результатам и целесообразно установить $n = 3$ при линейном порядке формирования группы.

Оценим стойкость метода по отношению к стегоанализу. Сначала оценим процент возникновения ошибок первого рода для тестовых наборов (A и B) пустых контейнеров (табл. 2).

Таблица 2

RS-анализ на наборе пустых контейнеров

L	0 %	1-4 %	5 % и более
Набор A	15 %	64 %	21 %
Набор B	16 %	79 %	5 %

То есть 21 % файлов для набора A и 5 % для набора B дают ошибку первого рода. Заполним контейнеры с помощью известных стегопрограмм HIDE4PGP и STEGOTOOLS. Процент заполнения контейнеров в данном эксперименте был установлен соответственно указанному ранее среднему проценту заполнения с целью сравнения результатов RS-анализа для разработанного нами метода и для указанных программ при равных процентах заполнения. В табл. 3 приведены результаты стегоанализа для контейнеров, заполненных с помощью программ HIDE4PGP и STEGOTOOLS.

Таблица 3

RS-анализ на наборе заполненных контейнеров

L	0 %	1-4 %	5 % и более
HIDE4PGP, набор A	0 %	0 %	100 %
HIDE4PGP, набор B	0 %	0 %	100 %
STEGOTOOLS, набор A	0 %	3 %	97 %
STEGOTOOLS, набор B	0 %	0 %	100 %

По данным табл. 3 видно, что RS-анализ обнаруживает наличие встроенной информации в 100 % случаев. Заполним контейнеры по предложенному методу и подвергнем их RS-анализу (табл. 4).

Таблица 4

RS-анализ на наборе заполненных контейнеров

L	0%	1-4%	5% и более
Набор A	15%	65%	20%
Набор B	15%	75%	10%

Результаты стегоанализа, приведенные в табл. 2 и 4, свидетельствуют о том, что процент обнаружения встроенной информации по предложенному методу практически идентичен проценту файлов, в которых имела место ошибка первого рода. Следовательно, можно утверждать, что метод устойчив к RS-атаке и может успешно использоваться. Таким образом, можно сделать вывод, что при уровне внедрения информации до 34 % от емкости не удается надежно отличить заполненный контейнер от пустого.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Рябко Б.Я., Рябко Д.Б.* Асимптотически оптимальные совершенные стеганографические системы // Проблемы передачи информации. – 2009. – Т. 45. – Вып. 2.
2. *Fridrich J., Goljan M., Du R.* Reliable detection of LSB steganography in color and grayscale images". Proc. of the ACM Workshop on Multimedia and Security, Ottawa, Canada, October 5, 2001. – P. 27-30.
3. *Жилкин М.Ю.* Теоретико-информационные методы стегоанализа графических данных: дисс. … канд. техн. наук. – Новосибирск, 2009.
4. *Грибунин В.Г., Оков И.Н., Туринцев И.В.* Цифровая стеганография. – М.: «Солон-Пресс», 2002. – 272 с.

Елтышева Екатерина Юрьевна
Сибирский государственный университет телекоммуникаций и информатики.
E-mail: Katya@1nsk.ru.
630102, г. Новосибирск, ул. Кирова 86.
Тел.: +79232455562.

Фионов Андрей Николаевич
E-mail: a.fionov@ieee.org.
Тел.: +73832698272

Yoltysheva Katherina Yur'evna
Siberian State University of Telecommunications and Informatics.
E-mail: Katya@1nsk.ru.
86, Kirova street, Novosibirsk, 630102, Russia.
Phone.: +79232455562.

Fionov Andrei Nikolaevich
E-mail: a.fionov @ ieee.org.
Phone: +73832698272.