Динамический способ стеганографического встраивания информации на основе LSB

И. А. Кривошеев, М. А. Линник

Хабаровский Федеральный исследовательский центр Дальневосточного отделения РАН,
г. Хабаровск, Россия

Аннотация. В работе предложен новый способ стеганографического сокрытия информации на основе метода LSB. Предлагается динамический алгоритм встраивания информации в цветное изображение, с учетом особенностей переходных характеристик отдельных блоков. Численным моделированием оценены возможности данного алгоритма противостоять атакам с использованием различных методов стегоанализа. Результаты экспериментальных исследований показали эффективность предложенного метода. Данный алгоритм может быть применен для встраивания информации в изображения форматов без сжатия информации.

Ключевые слова: стеганография, стегоконтейнер, стегоанализ, детерминант, LSB, RS-стегоанализ, Хи-квадрат стегоанализ, анализ битовых срезов.

DOI 10.14357/20718632220303

Введение

Вопрос защиты постоянно накапливаемого объема информации стоит очень остро, т.к. постоянно требуется обеспечивать высокий уровень конфиденциальности данных, для того чтобы быть уверенным в том, что передаваемая информация не попадет в руки третьих лиц. Одним из перспективных направлений решения такой задачи является использование методов стеганографии [1-3]. В настоящее время этот подход активно развивается и может быть использован для решения проблем защиты информации. Особенностью стеганографии является то, что объект, в который встраивается конфиденциальная информация (стегоконтейнер), не вызывает подозрений, из-за того, что он повторяет оригинал по своей структуре и внешнему виду. Таким образом, стеганография позволяет передавать информацию, скрывая факт ее существования.

Под сокрытием существования информации имеется в виду то, что в перехваченном контейнере наличие посторонней информации нельзя обнаружить без специальных методов оценки. Кроме того дешифрование извлеченных данных является трудно осуществимым или невозможным. В последнем случае проблема информационной безопасности возвращается к стойкости криптографического кода и можно сказать, что стеганография дополняет криптографию.

При использовании стеганографии следует обратить внимание, как на величину встраиваемых данных, так и на сами методы встраивания.

Обозначенный вопрос относится к проблеме пропускной способности. Иными словами, анализируется вопрос о допустимом объеме информации, который можно встроить в цветное изображение, таким образом, чтоб внесенные изменения нельзя было обнаружить.

На сегодняшний день разработано множество методов для стеганографического встраи-

вания, однако самым распространенным из них является метод замены наименее значимого бита в цветных изображениях (least significant bit – LSB) [4, 5]. При применении данного метода численное значение цвета преобразуется в двоичные биты и далее происходит замена последних знаков, как элементов, несущих незначительную информацию, которой можно пренебречь. У данного метода есть большие преимущества во встраиваемом объеме и скорости работы [6], но также имеется ряд ограничений, связанных, например, со стойкостью к атакам стегоанализа.

1. Постановка задачи

При использовании методов скрытия информации в пространственной области [1] одним из основных носителей информации является значение цвета пикселя. Существует несколько методик определения значения цвета пикселя. В данной работе рассматривается цветовое пространство RGB. В нем пиксель представляется в виде сочетания трех компонент цвета: красной (R), зеленой (G) и синей (B).

Значение каждой из компонент представляется в виде числа от 0 до 255, при использовании восьми разрядного двоичного кодирования, согласно которому число можно представить в двоичном виде. Последний символ (бит) числа в данном представлении несет минимум информации, потому что заключает в себе изменение значения пикселя на единицу. Такое искажение цвета не воспринимается глазом человека и поэтому может использоваться для встраивания. В этом случае допустимо использовать один или несколько последних символов двоичного числа для передачи информации. Однако, несмотря на гибкость и простоту данного алгоритма [7], у него существуют значительные недостатки. К ним относится отсутствие защищенности при малейших искажениях контейнера, так как секретная информация заложена в фактических значениях цвета. По этой причине классический метод LSB не работает с форматами изображения использующих сжатие (jpg, gif) [2].

Современное направление развития стеганографии включает в себя использование методов адаптивной стеганографии. Существуют ряд методов построения стегосистемы, в основе которых находится выделение маски наиболее значимых пикселей.

HUGO (Highly Undetectable steGO) [7] – минимизация влияния посторонней информации, которая достигается при использовании решетчатых кодов по алгоритму Витерби. Каждому пикселю присваивается определенный вес. Значение пикселя изменяется с вероятностью обратно пропорциональным его влиянию, которое определяется с помощью вычисленного значения веса.

WOW (Wavelet Obtained Weights) [8] – особенностью алгоритма является то, что в область окрестности пикселя, в которую встраивается информация, подвергается изменениям с целью скрыть влияние нарушения корреляционных связей между пикселями.

Их работа основана не только на встраивании информации, но и на минимизацию возникающих искажений после проведения анализа.

Кроме того, в области распознавания встроенной информации создаются новые методы на основе нейронных сетей, такие как, например, метод SPAM (Subtractive Pixel Adjacency Matrix) Features [9]. С помощью этого метода выявляются признаки, которые в дальнейшем используются для выполнения задачи классификации контейнеров на пустые и заполненные с помощью SVM-классификатора (Support Vector Machine) [10].

Указанные алгоритмы достаточно высокоэффективны, но они в своей работе требуют больших вычислительных мощностей, вследствие чего скорость их работы не высока. Кроме того из-за дополнительных ограничений снижается пропускная способность.

Отдельные попытки улучшения метода замены наименее значимого бита были предприняты в [4, 11-13]. Выбранное направление оказалось интересным, однако, полученные авторами результаты не позволяли говорить о полной защищенности и функциональности используемого метода. Поэтому перед исследователями по-прежнему стояла задача найти возможность усовершенствования метода как в сторону увеличения степени защищенности, так и быстродействия, не теряя пропускную способность.

2. Алгоритм разработанного метода

Суть предлагаемого способа [14] заключается в разбиении контейнера на специальные блоки. Однако в отличие от известного метода [4, 12], в данном методе изначально создается только один блок, который сдвигается попиксельно до тех пор, пока не будет обработано все изображение, т.е. динамическое представление блоков.

Предварительно, для работы алгоритма требуется выделить границы объектов изображения для исключения их из встраивания. Это делается для защиты от методов стегоанализа таких как, например, проверка битовых срезов. Такая операция позволяет избежать ситуации, когда контуры объектов будут стерты из-за добавления посторонней информации. Кроме того нарушение корреляционных связей между писклями будет проявляться слабее.

Для выполнения данной задачи был использован оператор выделения границ [15], позволяющий ясно выделить границы объектов, например, представленных на изображении (Рис. 1).

В каждом блоке, в свою очередь, проводится ряд преобразований с целью выявления наиболее подходящих блоков, которые будут использованы для встраивания информации. Для этого определяется модуль детерминанта каждого блока.

Предложенный метод позволяет снизить влияние граничных значений интенсивности цвета, которые являются наиболее нежелательными. Это преимущество возникает из-за того, что встраивание сообщения в эти точки будет происходить в последнюю очередь. Приоритетными будут считаться пиксели со средними значениями интенсивности цвета. Данный подход позволит повысить защиту от стеганографических атак и замаскировать факт встраивания информации.

На емкость стегоконтейнера накладываются дополнительные ограничения по причине того, что из общего количества разрешенных пикселей исключаются выявленные ранее границы объектов. Таким образом, количество информации, которое возможно встроить в контейнер, является индивидуальным для каждого изображения.

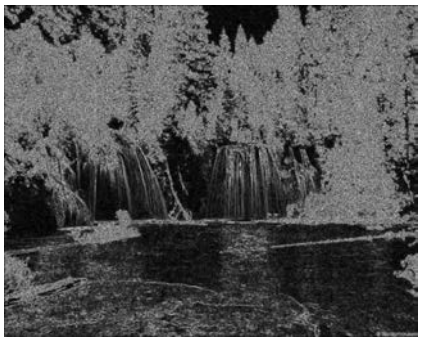


Рис. 1. Пример обработки изображения с помощью оператора выделения границ

Алгоритм предложенного способа можно представить следующим образом:

1) Формирование предварительной карты разрешенных пикселей. Для этого в изображении необходимо выделить границы объектов с помощью оператора выделения границ изображений.

2) Для однозначной оценки принадлежности к разрешенным или запрещенным пикселям необходимо перевести изображение из оттенков серого, получившегося после применения оператора выделения границ [15], в черно-белый формат.

3) В первоначальном контейнере формируется первый квадратный блок, выбранного размера. Чем меньше размер блоков, тем более точно будут учитываться особенности изображения (резкие перепады цвета и границы). Количество блоков вычисляется по формуле:

$$n = (h-(b-1))(w-(b-1)), \quad (1)$$

где w, h – ширина и высота изображения в пикселях, b – длина или ширина блока (в пикселях).

4) Формируется массив

$$A_k = \begin{bmatrix} a_{0,0},\ldots,a_{0,b-1} \\ \cdots,\quad a_{i,j},\quad \cdots \\ a_{b-1,0},\ldots,a_{b-1,b-1} \end{bmatrix},$$

где $k \in 0\ldots n$, n – количество блоков, $a_{i,j}$ – координаты пикселя в блоке, $i \in 0\ldots b\text{-}1$, $j \in 0\ldots b\text{-}1$, b – длина или ширина блока (в пикселях).

В нем размечаются как запрещенные (контуры объектов изображения), так и разрешенные пиксели. На Рис. 2 представлен пример получившейся итоговой карты, нанесенной на изображения, где черным показаны разрешенные пиксели.

а) б)

Рис. 2. Иллюстрация формирования карты разрешенных пикселей

а) исходное изображение; б) результирующая карта при использовании оператора выделения границ

5) Значение пикселя в сформированном блоке вычисляется по формуле [16]:

$$a_{i,j} = 0,299 * R + 0,587 * G + 0,114 * B \quad (2)$$

$i \in 0…b\text{-}1$, $j \in 0…b\text{-}1$ – координаты пикселя в блоке

$R \in 0…255$, $G \in 0…255$, $B \in 0…255$ – цветовые компоненты пикселя.

Затем выполняется математическое преобразование и выполняется вычисление значения модуля детерминанта $det|D_k|$, где $k \in 0…n$, n – количество блоков.

Полученное значение запоминается.

6) Происходит сдвиг блока на один пиксель вправо. При достижении границы ширины изображения выполняется переход на начало следующей строки изображения, и выполняется сдвиг на пиксель вниз. После этого продолжается формирование новых блоков.

На Рис. 3 представлена визуальная схема, показывающая сдвиг блоков на изображении.

7) Для нового блока повторяется шаг 5.

8) Действия, описанные в шагах 4-7, повторяются до тех пор, пока все изображение не будет охвачено.

9) Сформированный массив модулей детерминантов $S = \{det|D_0|, \dots, det|D_n|\}$ сортируется по убыванию.

10) На этом шаге происходит выбор пикселей для встраивания. Из массива модулей берется первый элемент и сверяется с массивом карт, полученном на шаге 4. Для встраивания выбирается первый разрешенный пиксель. Выбранный пиксель далее помечается как запрещенный. Это необходимо из-за наложения блоков друг на друга, и таким образом опасность использования задействованных в предыдущих блоках пикселей устраняется. Если же все пиксели заняты, то блок пропускается. Аналогичным образом анализируются все блоки из массива отсортированных значений.

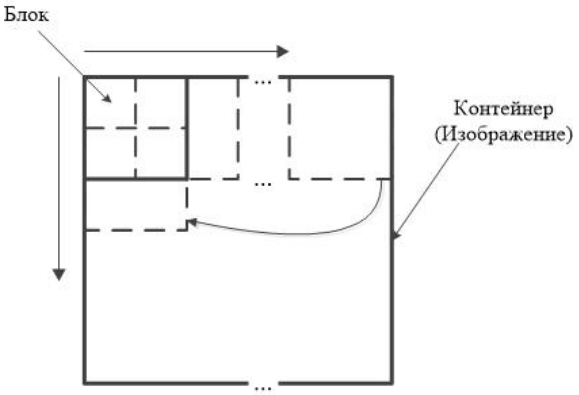


Рис. 3. Схема сдвига блоков на изображении

Таким образом, для встраивания используется только один пиксель в блоке.

11) Встраивание информации в выбранный пиксель происходит в последние младшие биты пикселя по методу LSB во все три компоненты цвета: красную, синюю и зеленую.

На Рис. 4 приведена схема работы алгоритма.

При извлечении повторяются шаги 1-10. После формирования карты расположения пикселей происходит обход изображения по полученным координатам и сбор битов секретной информации.

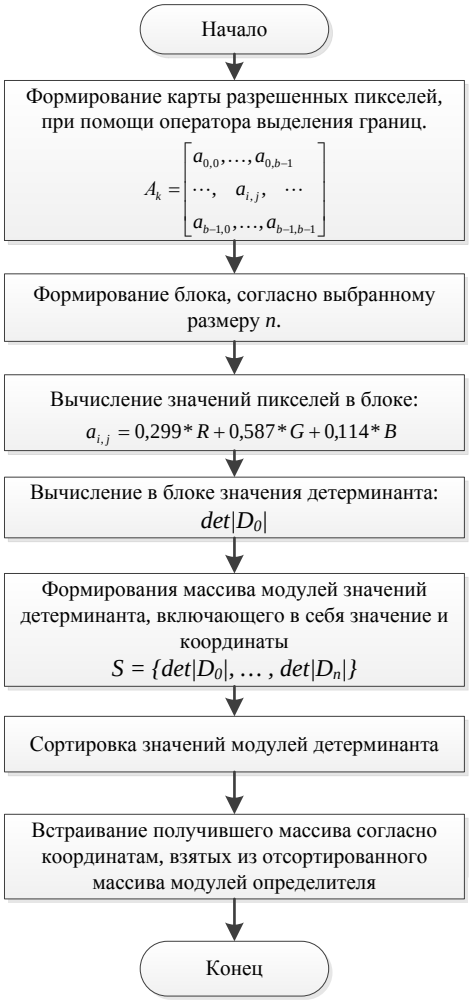


Рис. 4. Схема работы алгоритма

Максимальный объем информации, который можно встроить в изображение для блока выбранного размера, вычисляется по формуле:

$$V = 3(h-(b-1))(w-(b-1)) - \sum z \quad (3)$$

где b – длина или ширина блока; w, h – ширина и высота изображения в пикселях; $\sum z$ – сумма запрещенных для встраивания пикселей.

3. Численное моделирование

Для проведения экспериментов была взята группа из десяти изображений размера 1024x1280 пикселей. Для того чтобы в группе отличать одно изображение от другого необходимо выбрать какой-то параметр. Такие параметры известны в литературе [1, 13]. Однако для таких вычислений требуется априорная информация о занятых пикселях, которой пока мы не располагаем.

В нашем случае изображения отбирались по ряду критериев. Рассматривалось их структурное и яркостное содержание, а также преобладание высоких или низких значений яркости цвета. Кроме того, для данного тестового набора отбирались экземпляры, содержащие либо большое, либо малое количество объектов.

Авторами был предложен идентификационный параметр, состоящий из отношения площади выбранных пикселей к общей площади пикселей в изображении. Ввод такой характеристики необходим для того, чтобы упорядочить изображения и ранжировать их согласно их пригодности в качестве стегоконтейнеров.

Введем ряд определений. Под областью пикселей понимается участок на изображении, все пиксели которого находятся в определенном диапазоне интенсивности цвета. Элемент принадлежит к рассматриваемой области, если как минимум с одной стороны рядом с ним находятся пиксели, принадлежащие такой же цветовой области.

Пиксель называется граничным, если элемент рядом с ним, принадлежит к другому диапазону цветовой области. Кроме того вводится следующее ограничение: одиночные пиксели (изолированные), то есть элементы со всех сторон окруженные пикселями, принадлежащими к другим цветовым областям, не рассматриваются в вычислении параметра.

Для рассмотрения была выбрана область самых высоких значений интенсивности от 170 до 255. Иными словами анализируются колебания в ярких областях цвета.

Идентификационный параметр вычисляется по формуле 4:

$$Sq = \frac{\sum p}{w \cdot h - \sum p'}, \quad (4)$$

где $\sum p$ – сумма пикселей в области рассматриваемого диапазона; $\sum p'$ – сумма изолированных пикселей; w, h – ширина и высота изображения.

На основе предложенного идентификационного параметра были рассчитаны численные значения для выбранной группы (Табл. 1).

Табл. 1. Ранжирование группы изображений

№ изображения	1	2	3	4	5	6	7	8	9	10
Sq (10^{-5})	1	2	6	7	39	72	83	89	121	128

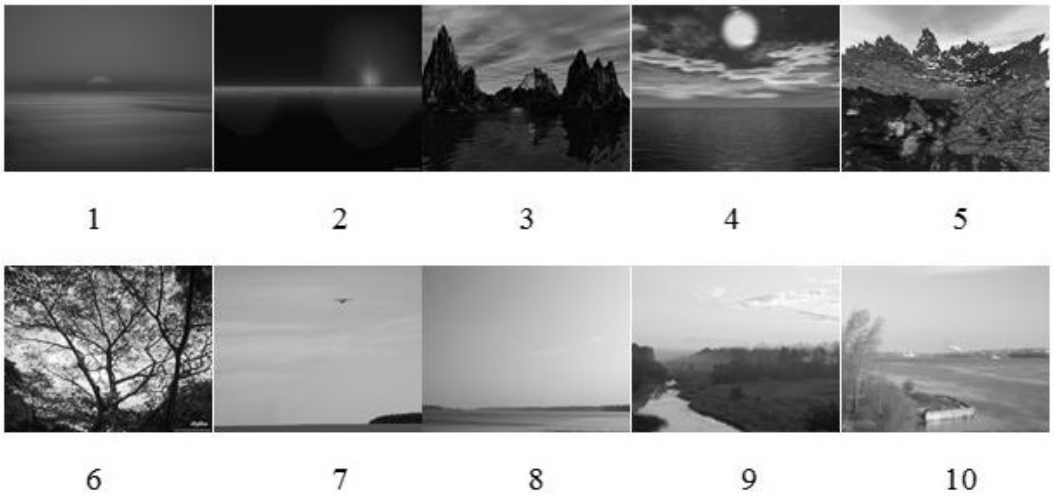


Рис. 5. Группа отсортированных изображений

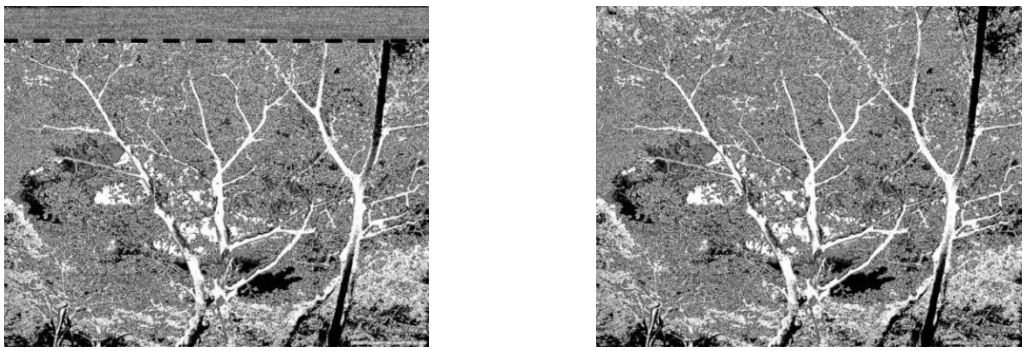
На Рис. 5 показана выбранная группа изображений, отсортированная по возрастанию идентификационного параметра для каждого из них.

Для проведения экспериментов в изображения были встроены 10%, 30% и 50% информации от общего допустимого объема с помощью метода LSB и разработанного алгоритма.

Для проверки работоспособности алгоритма были выполнены атаки несколькими способами стегоанализа, и оценивались полученные результаты на предмет защищенности от обнаружения факта встраивания информации.

Рассмотрим атаку стегоанализом с использованием метода оценки битовых срезов [17]. На Рис. 6 показаны битовые срезы изображений, в которые встраивалась информация методом LSB и предлагаемым методом. Количество встроенной информации в обоих случаях было одинаково. Процент внедряемой информации вычисляется от максимального объема, который возможно встроить согласно методу LSB.

На данном рисунке видно, что при применении классического метода LSB посторонние данные четко видны. Однако в случае использования



а) б)

Рис. 6. Битовый срез контейнеров с 10% внедренной информацией

а) LSB, б) предложенного способа

предложенного алгоритма передаваемое сообщение рассеяно по определенным участкам контейнера и из-за этого незаметно. Таким образом, разработанная модификация защищена от воздействия данного способа стегоанализа.

Далее рассмотрим широко известные статистические способы стегоанализа. Работа этих алгоритмов опирается на статистические зависимости между распределением пикселей в изображении.

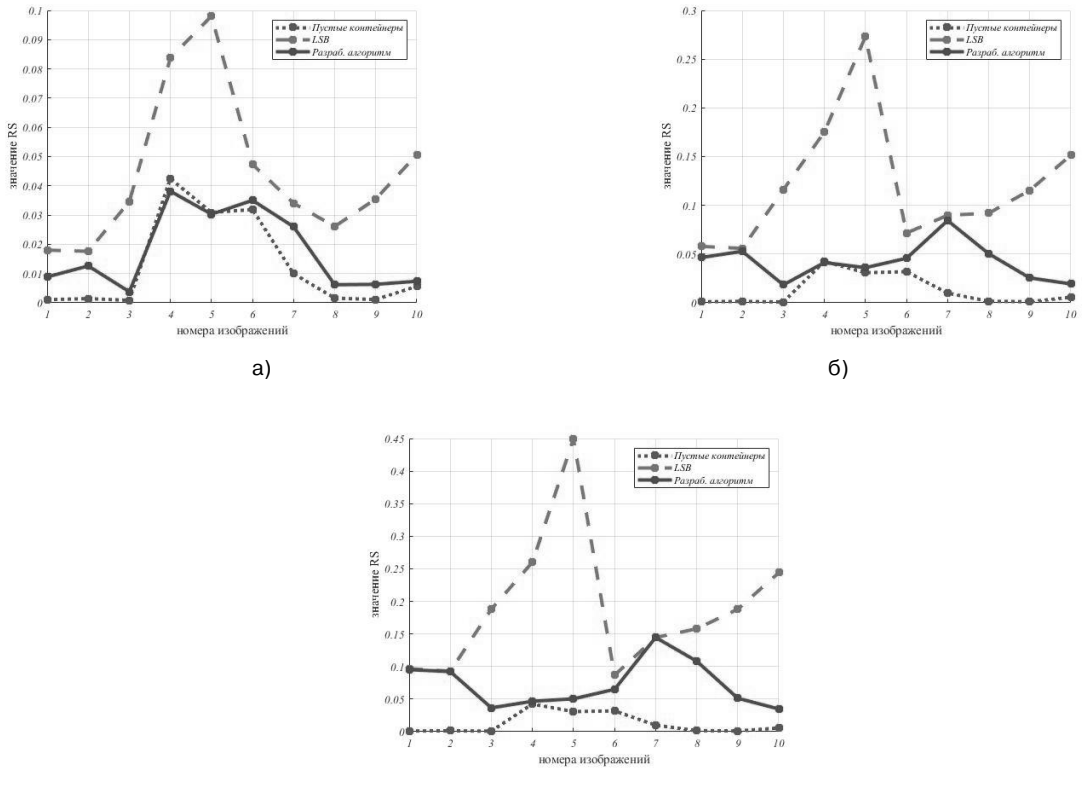
В случае RS-стегоанализа пиксели изображения разбиваются на группы, к ним применяются процедуры флиппинга с применением введенной маски и дискриминант-функции [18]. После выполнения необходимых вычислений анализируются полученные значения этой функции до и после применения процедуры флиппинга.

Алгоритм основывается на предположении равенства регулярных и сингулярных групп в пустом изображении после применения процедуры флиппинга. В ином случае предполагается, что в изображении встроена информация.

На Рис. 7 изображены графики значений RS-стегоанализа, выполненных для 10 изображений со встроенной информацией разного объема. Величина RS, получившаяся в результате вычислений, показывает с некоторой погрешностью долю измененных пикселей изображения от общего числа возможных [18, 19].

Из приведенных графиков видно, что во всех случаях полученное значение RS-стегоанализа для предложенного способа ниже, чем аналогичное в стандартном методе LSB. Кроме того, в ряде случаев оно принимает крайне низкое значение, которое можно принять за погрешность.

Следующий способ стегоанализа использует в своей работе критерий Хи-квадрат [5]. Этот метод основывается на предположении, что в



а) б)

в)

Рис. 7. Результаты численного моделирования с использованием RS-стегоанализа для пустого контейнера, LSB и предложенного алгоритма

а) при заполнении 10% объема контейнера, б) при заполнении 30% объема контейнера, в) при заполнении 50% объема контейнера

пустом контейнере цвета распределяются согласно тому, что вероятность одновременного появления соседних цветов, то есть тех, которые различаются на один младший бит, незначительна. Если наблюдается противоположная картина, значит перед нами контейнер, содержащий посторонние данные.

На Рис. 8 представлены графики, показывающие значения распределения Хи-квадрат на изображениях при использовании стандартного встраивания методом LSB и разработанного алгоритма в случае встраивания различного объема информации. Значения указывают на процентное содержание количества групп (под группой понимается строка в изображении), где значение данного метода стегоанализа больше 90%.

В этом случае из анализа приведенных графиков (Рис. 7 и 8) видно, что во всех рассмотренных вариантах разработанный алгоритм показал более высокие результаты защищенности и при этом значения полученные данным методом весьма низкие, что дает возможность принять их за погрешность.

Кроме того значения стегоанализа у пустых изображений и стегоконтейнеров, заполненных с помощью разработанного алгоритма, совпадают даже при встраивании 50% информации от общего объема. Это свидетельствует о том, что метод хорошо маскирует передаваемые данные.

Заключение

В статье приведен динамический способ встраивания информации в цветные изображения методом LSB. Приведен алгоритм встраивания информации. Выявлено, что результат сокрытия информации существенно зависит от контейнера, то есть от самого цветного изображения. Для установления отличия одного изоб-

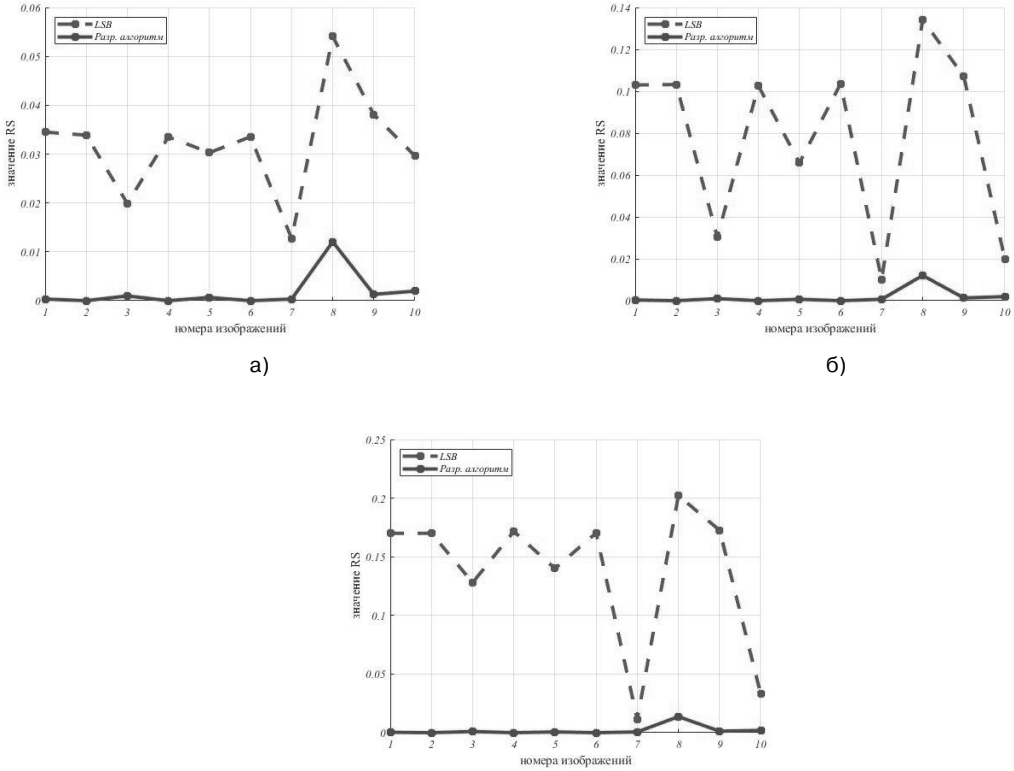


Рис. 8. Результаты численного моделирования для стегоанализа с использованием критерия Хи-квадрат для LSB и предложенного алгоритма

а) при заполнении 10% объема контейнера, б) при заполнении 30% объема контейнера, в) при заполнении 50% объема контейнера

ражения от другого был разработан идентификационный параметр, согласно которому ранжировались изображения. Численным моделированием было показано существенное преимущество предложенного способа от известных аналогов. Согласно результатам стегоанализа широко известных способов можно предположить, что в предложенном варианте заметно увеличилась стегостойкость и увеличилась вероятность того, что контейнер с встроенными данными не будет дискредитирован, иначе говоря, факт передачи информации не будет обнаружен.

Итоги приведенных исследований и анализа предложенного алгоритма можно свести к следующим положениям. Предложенный алгоритм выгодно отличается от известных: во-первых, тем, что объем встраиваемой информации может быть увеличен. Во-вторых, предложенный алгоритм адаптируется к каждому стегоконтейнеру независимо от размера встраиваемой информации. В-третьих, не все широко известные алгоритмы анализа могут обнаружить передаваемое сообщение в силу невосприимчивости встраивания предложенным способом.

Результатами численного моделирования установлено, что, предложенный способ встраивания достаточно хорошо позволяет скрыть передачу данных, несмотря на произведенные атаки различные методами.

Из проведенных экспериментов видно, что алгоритм полностью защищен от стегоанализа по методу изучения битовых срезов, RS-стегоанализа, стегоанализа на основе критерия Хи-квадрат, при условии, что встраиваются небольшие объемы информации (до 30% от максимально возможного).

К преимуществам разработанного алгоритма можно отнести и то, что выбор каждого контейнера осуществляется индивидуально, что позволяет проявить гибкость к процессу встраивания.

Кроме того, в сравнении с методами, представленными в [15, 20], данный алгоритм имеет преимущество в объеме встраиваемой информации и скорости работы.

Относительно [4, 14] расчетные значения у рассмотренных методов стегоанализа ниже, чем у разработанного метода, что свидетельствует о повышении защищенности стегосистемы.

Особо следует подчеркнуть, что эффективность работы алгоритма зависит от особенностей изображения, которое учитывается разработанным идентификационным параметром.

Литература

1. Коханович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. К.: МК-Пресс. 2006. 288 с.
2. Абазина, Е.С. Цифровая стеганография: состояние и перспективы // Системы управления, связи и безопасности. Санкт-Петербург: БГТУ, 2016. № 2. С. 182-201.
3. Грибунин В.Г., Оков И.Н. Цифровая стеганография. М.: Солон-пресс. 2002. 272 с.
4. Кривошеев И.А., Линник М.А. Статический способ стеганографического встраивания информации на основе LSB // Системы и средства информатики. 2020. Т. 30, № 3. С. 56-66.
5. Westfield A., Pfitzmann A. Attacks on Steganographic Systems Breaking the Steganography Utilities EzStego, Jsteg, Steganosand S-Tools and Some Lessons Learned // Dresden University of Technology, Department of Computer Science, Information Hiding, Third International Workshop, IH'99 Dresden Germany, September. 1999. pp. 61-76.
6. Urbanovich N., Plaskovitsky V. The use of steganographic techniques for protection of intellectual property rights // New Electrical and Electronic Technologies and Their Industrial Implementation: 7th Conference (International). 2011. pp. 147-148.
7. Pevny T., Filler T., Bas P. Using High-Dimensional Image Models to Perform Highly Undetectable Steganography / T. Pevnýˊ, T. Filler, P. Bas // Information Hiding. 2010. pp. 161-177.
8. Holub V., Fridrich J. Designing Steganographic Distortion Using Directional Filters // Proc. 4th IEEE Intern. Workshop on Inform. Forensics and Security (WIFS). 2012. pp. 234-239.
9. Pevny T., Bas P., Fridrich J. Steganalysis by subtractive pixel adjacency matrix // IEEE Transactions on Information Forensics and Security. 2010. 5(2). pp. 215-224.
10. Wang P., Wei Z., Xiao L. Pure spatial rich model features for digital image steganalysis // Multimedia Tools and Application. 2015. 75(5). pp. 2897–2912..
11. Кривошеев И.А., Линник М.А., Кожевникова Т.В. Способ встраивания информации в цветное изображение // Патент РФ на изобретение №2738250 от 26.03.2020. Бюл. № 35.
12. Дрюченко М.А., Сирота А. А. Алгоритм стеганографическогого скрытия информации на основе пространственной деформации фрагментов полноцветных изображений. // Компьютерная оптика. 2014. Т. 38, № 4. С. 833-842.
13. Кривошеев И.А., Линник М. А. К вопросу об оценке устойчивости стеганографической системы // Ученые заметки ТОГУ. 2017. Т. 8, № 2. С. 433-437.
14. Кривошеев И.А., Линник М.А., Способ встраивания конфиденциальной информации в цветное изображе-

ние // Патент РФ на изобретение № 2749880 от 18.06.2021. Бюл. № 17.
15. Анисимов Б.В. Распознавание и цифровая обработка изображений. М.: Высш. школа. 1983. 295 с.
16. Гонсалес Р., Вудс Р. Цифровая обработка изображений. М. Техносфера. 2005. 1072 с
17. Pfitzmann A., Westfeld A. Attacks on Steganographic Systems. Breaking the Steganographic Utilities EzStego, Jsteg, Steganos, and S-Tools and Some Lessons Learned. IH 1999. LNCS, 1768: pp. 61-76.
18. Fridrich J., Goljan M., Du R. Reliable Detection of LSB Steganography in Color and Grayscale Images // State Univ. of New York, Binghamton, NY, USA. 2001. pp. 27-30
19. Fridrich J., Du R., Meng L. Steganalysis of LSB Encoding in Color Images // IEEE International Conference on Multimedia and Expo: IEEE Computer Society Press. 2000. Vol.3. pp. 1279-1282.
20. Евсютин О.О. Модификация стеганографического метода LSB, основанная на использовании блочных клеточных автоматов // Инофрматика и системы управления. 2014. Т. 39, № 1. С. 15-22.

Кривошеев Игорь Александрович. Хабаровский Федеральный исследовательский центр Дальневосточного отделения РАН г. Хабаровск, Россия. Главный научный сотрудник, доктор технических наук. Количество печатных работ: 151. Область научных интересов: информационная безопасность и защита информации, численное моделирование, обработка изображений. E-mail: igork@as.khb.ru

Линник Максим Анатольевич. Хабаровский Федеральный исследовательский центр Дальневосточного отделения РАН г. Хабаровск, Россия. Младший научный сотрудник. Количество печатных работ: 12. Область научных интересов – информационная безопасность, численное моделирование, обработка изображений. E-mail: linnik.max1995@mail.ru

Dynamic Algorithm of Steganographic Information Embedding Based on LSB

I. A. Krivosheev, M. A. Linnik

Khabarovsk Federal Research Center of the Far Eastern Branch of the Russian Academy of Sciences, Khabarovsk, Russia

Abstract. The paper proposes a new method of steganographic information hiding based on the LSB method. A dynamic algorithm for embedding information into a color image is proposed, taking into account the peculiarities of the transient characteristics of individual blocks. Numerical modeling was used to evaluate the capabilities of this algorithm to resist attacks by various methods of steganalysis. The results of experimental studies have shown the advantage of this algorithm. This algorithm can be used to embed information in image formats without information compression.

Keywords: steganography, stego-carrier, stegoanalysis, determinant, LSB, RS-steganalysis, Chi-square stegoanalysis, bit-slice analysis.

DOI 10.14357/20718632220303

References

1. Kokhanovich, GF, Puzyrenko, A.Y. 2006. Komp'juternaja steganografija. Teorija i praktika [Computer steganography. Theory and practice.]. K.: MK-Press,. 288 p.
2. Abazina, E.S. 2016. Cifrovaya steganografiya: sostoyanie i perspektivy [Digital steganography: state of the art and prospects]. Sistemy upravleniya, svyazi i bezopasnosti [Control Systems, Communications and Security]. № 2: 182-201.
3. Gribunin, V.G., Okov, I.N. 2002. Cifrovaja steganografija [Digital steganography] Moskow: Solon-press. 272 p.
4. Krivosheev, I.A., Linnik, M.A. 2020. Staticheskij sposob steganograficheskogo vstraivanija informacii na osnove LSB [Static way of steganographic information embedding based on LSB]. Sistemy i sredstva informatiki [Systems and Means of Informatics]. 30(3): 56-66.
5. Westfield A., Pfitzmann A. Attacks on Steganographic Systems Breaking the Steganography Utilities EzStego, Jsteg, Steganosand S-Tools and Some Lessons Learned // Dresden University of Technology, Department of Computer Science, Information Hiding, Third International Workshop, IH'99 Dresden Germany, September. 1999. pp. 61-76.
6. Urbanovich N. Plaskovitsky V. The use of steganographic techniques for protection of intellectual property rights // New Electrical and Electronic Technologies and Their Industrial Implementation: 7th Conference (International). 2011. pp. 147-148.

7. Pevny T. Filler T., Bas P. Using High-Dimensional Image Models to Perform Highly Undetectable Steganography / T. Pevný, T. Filler, P. Bas // Information Hiding. 2010. pp. 161-177.
8. Holub V. Designing Steganographic Distortion Using Directional Filters // Proc. 4th IEEE Intern. Workshop on Inform. Forensics and Security (WIFS). 2012. pp. 234-239.
9. Pevny T. Bas P., Fridrich J. Steganalysis by subtractive pixel adjacency matrix // IEEE Transactions on Information Forensics and Security. 2010. 5(2). pp. 215-224.
10. Wang P., Wei Z., Xiao L. Pure spatial rich model features for digital image steganalysis // Multimedia Tools and Application. 2015. 75(5). pp. 2897–2912.
11. Krivosheev, I.A., Linnik, M.A.., Kozhevnikova T.V. 2020. Sposob vstraivanija informacii v cvetnoe izobrazhenie [Method of embedding information into a color image]. Patent RF No. 2738250.
12. Dryuchenko M.A., Sirota A. A. 2014. Algoritm steganograficheskogogo skrytiya informacii na osnove prostranstvennoj deformacii fragmentov polnocvetnyh izobrazhenij [Steganographic information hiding algorithm based on spatial deformation of full-color image fragments]. Komp'yuternaya optika [Computer optics]. 38(4): 833-842.
13. Krivosheev I.A., Linnik M.A. 2021. Sposob vstraivaniya konfidencial'noj informacii v cvetnoe izobrazhenie [Method for embedding confidential information in a color image]. Patent RF No. 2749880.
14. Krivosheev, I.A., Linnik, M.A. 2017. K voprosu ob otsenke ustoychivosti steganograficheskoy sistemy [On the issue of assessing the stability of a steganographic system]. Uchenye zametki TOGU [TOGU Science Notes]. 8(2): 433-437.
15. Anisimov, B.V. 1983. Raspoznavanie i cifrovaja obrabotka izobrazhenij [Recognition and digital processing of images]. Moskow.: High School. 295 p.
16. Gonzalez R., Woods R. Tsifrovaya obrabotka izobrazheniy [Digital image processing]. Moskow: Tekhnosfera. 1072 p.
17. Pfitzmann, A., Westfeld, A. Attacks on Steganographic Systems. Breaking the Steganographic Utilities EzStego, Jsteg, Steganos, and S-Tools and Some Lessons Learned. IH 1999. LNCS, 1768: pp. 61-76
18. Fridrich J., Goljan M., Du R. Reliable Detection of LSB Steganography in Color and Grayscale Images // State Univ. of New York, Binghamton, NY, USA. 2001. pp. 27-30.
19. Fridrich J., Du R., Meng L. Steganalysis of LSB Encoding in Color Images // IEEE International Conference on Multimedia and Expo: IEEE Computer Society Press. 2000. Vol.3. pp. 1279-1282.
20. Evsyutin O.O. 2014. Modifikaciya steganograficheskogo metoda LSB, osnovannaya na ispol'zovanii blochnyh kletochnyh avtomatov[Modification of the LSB steganographic method based on the use of block cellular automata]. Inofrmatika i sistemy upravleniya [Inofrmatika and control systems]. 39(1): 15-22.

Krivosheev I. A. Doctor of Science in technology, leading scientist, Khabarovsk Federal Research Center of the Far Eastern Branch of the Russian Academy of Sciences, Turgeneva street, 51, Khabarovsk, 680000 Russia, e-mail: igork@as.khb.ru.

Linnik M. A. Junior scientist, Khabarovsk Federal Research Center of the Far Eastern Branch of the Russian Academy of Sciences, Turgeneva street, 51, Khabarovsk, 680000 Russia, e-mail: linnik.max1995@mail.ru