Прикладная математика & Физика, 2024, том 56, № 4. С. 328–336.
Applied Mathematics & Physics, 2024, Volume 56, No 4. P. 328–336.

УДК 519.72
MSC 68W99, 94A60, 94B99
Оригинальное исследование
DOI 10.52575/2687-0959-2024-56-4-328-336

Модификация стеганографического метода неравномерных смещений с учетом особенностей сегментов графического контейнера

Твердохлеб В. В., **Хлопов А. М.**, **Акиньшин Д. И.**
(*Статья представлена членом редакционной коллегии Ю. П. Вирченко*)

[1] Белгородский государственный технологический университет им. В. Г. Шухова,
Россия, 308012, г. Белгород, ул. Костюкова, 85
akinsindaniL7@icloud.com

Аннотация. Анализируется концепция построения модифицированного стеганографического метода неравномерных смещений, реализуемого в LSB-области контейнера. При этом в качестве контейнера рассматривается изображение формата Jpeg. Разрабатываются механизмы гибкой смены шага смещения и его направления исходя из выявленных статистических характеристик фрагмента контейнера. Описывается возможная проблематика реализации предлагаемых механизмов, а также пути ее устранения.

Ключевые слова: контейнер, хроматические пространства, инкапсуляция, яркостные компоненты

Для цитирования: Твердохлеб В. В., Хлопов А. М., Акиньшин Д. И. 2024. Модификация стеганографического метода неравномерных смещений с учетом особенностей сегментов графического контейнера. *Прикладная математика & Физика*, 56(4): 328–336. DOI 10.52575/2687-0959-2024-56-4-328-336

Original Research

Modification of the Steganographic Method of Irregular Displacements, Taking into Account the Features of the Segments of the Graphic Container

Vitalii V. Tverdokhleb, **Andrey M. Khlopov**, **Danil I. Akinshin**
(*Article submitted by a member of the editorial board Yu. P. Virchenko)*

Belgorod State Technological University named after V. G. Shukhov,
85 Kostyukova St., Belgorod 308012, Russia
akinsindaniL7@icloud.com

Abstract. The concept of constructing a modified steganographic method of irregular displacements implemented in the LSB region of the container is analyzed. At the same time, a Jpeg image is considered as a container. Mechanisms for flexible change of the displacement step and its direction are being developed based on the identified statistical characteristics of the container fragment. The possible problems of the implementation of the proposed mechanisms, as well as ways to eliminate them, are described.

Keywords: Container, Chromatic Spaces, Encapsulation, Brightness Components

For citation: Tverdokhleb V. V., Khlopov A. M., Akinshin D. I. 2024. Modification of the Steganographic Method of Irregular Displacements, Taking into Account the Features of the Segments of the Graphic Container. *Applied Mathematics & Physics*, 56(4): 328–336. (in Russian) DOI 10.52575/2687-0959-2024-56-4-328-336

1. Введение. Информационная среда в нынешнем виде характеризуется существованием множества рисков, сопряженных с возможностью хищения или несанкционированной модификации конфиденциальных данных. В частности, это замечание актуально для ситуации обмена данными с ограниченным доступом открытыми каналами. Традиционно, для того, чтобы либо минимизировать, либо полностью исключить вероятность получения и дальнейшего использования такой информации посторонними лицами, используются различные криптографические системы. Вместе с тем сейчас складываются условия, когда, с одной стороны, злоумышленник располагает достаточными вычислительными ресурсами, а, с другой стороны, разработчик формально подходит к реализации той или иной шифросистемы. Кроме того, за последние несколько лет в сфере криптографии отсутствуют принципиально новые решения, которые получили бы широкую практическую реализацию. В этом случае возможной альтернативой шифрованию данных является их сокрытие на основе стеганографических алгоритмов. Такой подход имеет неоспоримое преимущество по сравнению с использованием криптографии ввиду отсутствия конкретного объекта атаки [1, 2]. Однако в настоящее время единые стандарты стеганографии отсутствуют, а большинство классических алгоритмов в их базовой реализации не обеспечивают достаточного уровня стойкости. В связи с этим целесообразным является выполнить доработку одной из наиболее

классических разработок в сфере стеганографии, а именно, усовершенствование метода неравномерных смещений [1, 3].

2. Постановка задачи. Стеганографические методы передачи информации обеспечивают построение скрытых каналов обмена данными, что может рассматриваться альтернативой криптографическим методам защиты. Однако, в отличие от шифрованных каналов, наличие скрытых каналов злоумышленнику заранее неизвестно, что является неоспоримым преимуществом скрытой передачи [1]. При этом основой идеологии скрытой передачи данных является концепция «контейнер-метод». Здесь контейнером является файл (совокупность файлов), в который встраиваются скрываемые данные. В свою очередь, в рамках общей идеологии стеганографии, инкапсуляцией является встраивание фрагментов (бит, байт и т. д.) скрываемого сообщения в контейнер.

В настоящее время одним из перспективных направлений развития методов стаганографии является LSB-стеганография (т. е. стеганография с использованием пространства младших бит символов сообщения в двоичном представлении). При этом классический подход LSB-стеганографии предполагает, что встраивание производится последовательно и побитно начиная либо с начальной координаты $(0;0)$, либо с произвольной координаты контейнера. Однако в этом случае применяется фротнальный способ встраивания – биты скрываемого сообщения инкапсулируются в LSB-пространство сплошным потоком. В свою очередь, LSB-пространство рассматривается, как совокупность наименее значимых бит (Less Significant Bit) контейнера в его двоичном описании. По умолчанию, это совокупность бит нулевого разряда контейнера.

В рамках реализации LSB-встраивания, согласно методу неравномерных смещений, инкапсуляция i-го бита скрываемого сообщения выполняется путем модификации бита из пространства наименее значимых бит (нулевой разряд) компонент $c_i(x;y)$ (i-я компонента с координатами $(x;y)$ в изображении) [1, 3]. Компонентой $c_i(x,y)$ здесь является десятичное значение яркостного Y, либо хроматического (Cb или Cr) канала, получаемое в результате выполнения процедуры смены цветовой палитры (процедура является стандартной для Jpeg). Вместе с тем процедура модификации выполняется следующим образом:

$$\begin{cases} b_{x,y}^{(0)} := b_{x,y}^{(0)} | b_i = b_{x,y}^{(0)}; \\ b_{x,y}^{(0)} := b_i | b_i \neq b_{x,y}^{(0)}, \end{cases} \tag{1}$$

где $b_{x,y}^{(0)}$ – бит нулевого разряда компоненты $c(x,y)$. Следовательно, согласно системе выражений (1), бит нулевого разряда на позиции $(x;y)$ остается неизменным при условии равенства с i-м битом b_i скрываемого сообщения, и наоборот. В свою очередь, вычисление актуального указателя $s_{(i+1)}$ смещения для этапа $(i+1)$ встраивания производится согласно следующему принципу:

$$s_{i+1} = \sum_{j=1}^{J-1} (b^{(j)} - 1 | b^{(j)} = 1), \tag{2}$$

где J – количество разрядов, необходимых для описания компоненты $c_i(x,y)$. Анализ выражения (2) показывает, что максимальный шаг $\Delta s_{\max}$ смещения в этом случае не будет превышать величину $(J-1)$.

Следовательно, существующая реализация метода предполагает выполнение обхода контейнера в направлении строк/столбцов с шагом $\Delta s_{\max} \leq (J-1)$ [3, 7]. С учетом того, что рассматриваемый метод не предусматривает наличие механизма выбора стартовой точки, складываются условия, в которых факт наличия контейнера может быть выявлен. Для этого воссоздаются и анализируются цепочки бит, получаемые путем сканирования LSB-последовательностей компонент $c_i(x,y)$ в диапазоне значений и $x = \overline{1;\ X}$, $y = \overline{1;\ Y}$, учитывая шаг $s_{(i+1)}$ по их месту.

Таким образом, чтобы обеспечить повышение уровня защищенности скрываемых данных, *требуется*:

1. разработать алгоритм выбора стартовой точки обхода контейнера без привязки к абсолютным координатам;

2. построить алгоритм выбора направления d обхода пространства LSB, принимая за основу существующий метод неравномерных смещений;

3. обеспечить возможности смещения шага записи на величину, существенно превышающую максимальное значение $\Delta s_{\max}$.

Разрабатываемые алгоритмы должны соответствовать следующим требованиям:

— простота и отсутствие существенной вычислительной нагрузки;

— нетривиальная реализация, что создает условия для возможности обеспечения защищенности стеганограмм;

— отсутствие необходимости или минимизация использования дополнительных служебных данных.

3. Общая концепция модификации метода неравномерных смещений. С учетом перечисленных требований к разрабатываемым алгоритмам: простоты, обеспечения защищенности стеганограмм и сведения к минимуму объема служебных данных, предлагается:

1. В ходе реализации каждого алгоритма учитывать особенности содержания сегментов контейнера. Для этого возможно использовать множество $\{\Theta\}$ статистических характеристик каждого из них.

2. Строить алгоритмы на основе параметрического подхода. В свою очередь, здесь требуется задействовать множества $\{\eta\}$ и $\{\mu\}$ параметрических величин. При этом $\{\eta\}$ предполагается использовать, как набор опций в ходе реализации сценария алгоритмов, тогда как $\{\mu\}$ используется в ходе вычисления элементов множества $\{\Theta\}$.

Множества $\{\eta\}$ и $\{\mu\}$ являются элементами стегоключа.

4. Построение механизма выбора направления обхода пространства контейнера. Контейнер F изначально рассматривается в виде двумерного массива $K \times L$ – размером сегментов $C(a;b)$. Здесь a и b – индексы сегмента в графическом контейнере. В свою очередь, сегмент формируется как двумерный массив компонент $c(m;n)^{(a,b)}$, где $m,n = \overline{1;8}$ – координаты компоненты в пределах сегмента, находящегося на позиции $a = \overline{1;K/8}$ и $b = \overline{1;L/8}$ [4, 5]. Иначе говоря, сегмент представляет собой матрицу 8×8 компонент.

Для возможности реализации механизма изменения направления обхода вместо шага Δs записи предлагается использовать вектор записи $V_w = (s;d)$. Под вектором записи понимается пара чисел $(c;d)$, где s – указатель смещения на следующую точку записи, d – направление смещения $(d \in Z)$. При этом, здесь $d \in \{1,2,3,4\}$, где каждое из чисел соответствует одному из направлений (вниз, влево, вверх, вправо), а согласно базовой реализации метода неравномерных смещений $s = \overline{1;7}$.

Принимая во внимание вышесказанное, отметим, что задача построения механизма изменения направления обхода пространства младших бит сводится к решению следующих подзадач:

— выбор пространства для реализации механизма;

— определение условий изменения направления смещения.

В рамках решения первой подзадачи необходимо выбрать пространство для реализации механизма. Для этого выполним анализ процесса JPEG-преобразований изображения [3, 4, 5]. При этом отметим, что каскад операций JPEG-базиса предполагает раздельную обработку пространства Y яркостных компонент и хроматических (цветоразностных) пространств – Cb (хроматические синие компоненты) и Cr (хроматические красные компоненты). Одним из технологических этапов обработки здесь является прореживание цветоразностных компонент (цветовая субдискретизация). Вследствие этого результирующая размерность хроматического пространства может быть существенно ниже, чем размерность пространства Y яркости [6, 7].

Таким образом, с точки зрения повышения потенциальной емкости контейнера имеет смысл выполнять встраивание данных в пространство яркостных компонент $c(m;n)^{(a,b)}$.

В рамках решения второй подзадачи предлагается использовать значение одной или ряда характеристик из множества $\{\Theta\}$, исходя из величин которых далее будет приниматься решение относительно направления смещения (значение переменной d).

В то же время смена направления смещения не должна носить детерминированный характер, что потенциально позволяет обеспечить уникальный итоговый маршрут обхода каждого контейнера, тем самым создавая условия для повышения защищенности стеганограмм.

Требуется также учитывать, что должна обеспечиваться возможность извлечения определенных статистических характеристик любого его сегмента $C(a;b)$, т. к. процесс обхода пространства младших бит должен осуществляться в пределах всего контейнера F. В то же время на данном этапе обработки контейнера F (яркостного пространства представления) его возможно рассматривать:

— на уровне совокупности компонент $c(m;n)^{(a,b)}$;

— на уровне массива сегментов $C(a,b)$.

Однако же для любой из компонент $c(m;n)^{(a,b)}$, по сути, являющей собой одно число, сформировать произвольное количество характеристик не представляется возможным. Соответственно, целесообразно выполнять расчет статистических характеристик сегментов контейнера.

Рассмотрим случай, когда решение относительно значения величины d принимается на основе одной из характеристик сегмента Θ_1. Предположим, что на произвольном i-м этапе работы алгоритма данная компонента $c(m;n)^{(a,b)}$ яркости подвергается процедуре встраивания данных. Тогда в процессе определения направления d смещения для фрагмента $C(a;b)$, которому принадлежит данная компонента,

вычисляется значение Θ_1 характеристики этого же сегмента в соответствии со следующей системой соотношений:

$$\begin{cases} d := 1 | \Theta_1 \in [\Theta_1^{(p)}; \eta_1 \Theta_1^{(p)}]; \\ d := 2 | \Theta_1 \in (\eta_1 \Theta_1^{(p)}; \eta_2 \Theta_1^{(p)}]; \\ d := 3 | \Theta_1 \in (\eta_2 \Theta_1^{(p)}; \eta_3 \Theta_1^{(p)}]; \\ d := 4 | \Theta_1 \in (\eta_3 \Theta_1^{(p)}; 0]; \end{cases} \tag{3}$$

где $\eta_1 > \eta_2 > \eta_3$, η_1, η_2 и η_3 – параметрические множители, которые могут принимать значения в диапазоне (0;1), их применение обеспечивает возможность гибкой конфигурации алгоритма. Данные величины предлагается использовать как элементы стеганографического ключа; $\Theta_1^{(p)}$ – пороговая величина характеристики Θ_1, определяемая по максимальному ее значению в пределах всех сегментов $C(a;b)$ контейнера F, а именно:

$$\Theta_1^{(p)} = \max\{\Theta_1(F)\}.$$

Иначе говоря, здесь величине d присваивается значение в зависимости от условия вхождения характеристики Θ_1 в тот или иной диапазон. Следовательно, исходя из системы соотношений (3), при $d = 1$ и $s = q$ для $(i+1)$-го этапа работы алгоритма далее используется компонента, отстоящая от компоненты $c(m;n)^{(a,b)}$ на $(-q)$ позиций по оси y, т. е. $c_{i+1}(m;n-q)^{(Ia,b)}$. Тогда общий принцип смещения может быть показан следующим образом:

$$c_{i+1}(m';n') = c_i(m;n) \cup V_w, \tag{4}$$

где $(m';n')$ – значение смещенной координаты компоненты относительно предыдущего этапа.

Если принять во внимание систему (3), то выражение (4) может быть представлено в более детальном виде, а именно:

$$\begin{cases} c_{i+1}(m';n') := c_i(m;n-q) | d = 1; \\ c_{i+1}(m';n') := c_i(m-q;n) | d = 2; \\ c_{i+1}(m';n') := c_i(m;n+q) | d = 3; \\ c_{i+1}(m';n') := c_i(m+q;n) | d = 4. \end{cases} \tag{5}$$

После того, как компонента $c_{i+1}(m';n')$, младший бит которой подлежит модификации, определена, действия, описываемые выражениями 1-3, повторяются для нее и всех последующих компонент, которые задействуются для встраивания бит скрываемого сообщения.

5. Разработка способа задания стартовой точки обхода контейнера. Чтобы создать условия для максимального затруднения выявления возможной стартовой точки встраивания в ходе стегоанализа, необходимо:

— обеспечить возможность установки координат стартовой точки в неявном виде;

— предусмотреть возможность осуществления выбора точки начала инкапсуляции таким образом, чтобы любую из координат $(m;n)$ возможно было выбрать с равной вероятностью;

— гарантировать однозначность определения стартовой точки $(m';n')$ на стороне приемника без использования дополнительной служебной информации.

С учетом сказанного выше, выбор стартовой точки обхода контейнера предлагается реализовать на основе следующего алгоритма.

Поскольку в роли контейнера рассматривается изображение Jpeg, его можно рассматривать как совокупность отдельных сегментов $C(a;b)$, где каждый сегмент представляет собой двумерный массив компонент. Это позволяет реализовать способ выбора точки старта за два шага, а именно, выполнить выбор сегмента $C(a;b)$, после чего выбрать ту или иную координату внутри ранее выбранного сегмента. В то же время выбор того или иного сегмента $C(a;b)$, а также координат m и n, может быть реализован по аналогии с механизмом выбора направления обхода пространства контейнера. Здесь также предлагается использовать пороговый подход на основе вычисления значений его статистических характеристик. Следовательно, на первом шаге для дальнейшего рассмотрения выбирается сегмент $C(a;b)$, для которого выполняется следующее условие:

$$\Theta_2 \in [\Theta_2^{(p)}; \eta_4 \Theta_2^{(p)}], \tag{6}$$

где η_4 – параметрический множитель, который может принимать значения в диапазоне величин (0;1); Θ_2 – значение одной из характеристик сегмента $C(a;b)$. При этом само значение $\Theta_2^{(p)}$, как и в случае $\Theta^{(p)}$, определяется следующим образом:

$$\Theta_2^{(p)} = \max\{\Theta_2(C(a;b))\}.$$

В свою очередь, в ходе реализации такого способа выбора сегмента может возникать ситуация неопределенности, когда условиям (6) удовлетворяет характеристика Θ_2 более чем одного сегмента. Иначе говоря, справедливо следующее выражение:

$$\{C(a;b)\} \subset [\Theta_2^{(p)}; \eta_4\Theta_2^{(p)}]. \tag{7}$$

В этом случае из полученного множества $\{C(a;b)\}$ сегментов предлагается принимать к дальнейшему рассмотрению такой, для индексов которого выполняется одно из соотношений:

$$(a = a_{\min}) \vee (b = b_{\min}) \vee ((a = a_{\min})|(b = b_{\min}))\,, \tag{8}$$

либо

$$(a = a_{\max}) \vee (b = b_{\max}) \vee ((a = a_{\max})|(b = b_{\max}))\,, \tag{9}$$

т. е. из множества $\{C(a;b)\}$ выбирается сегмент с минимальным (максимальным) значением одного или обоих индексов. Здесь, в случае обеспечения возможности выбора одного из режимов отбора индексов, указанных выражениями (8) и (9), соответственно появляется дополнительный механизм повышения защищенности процесса выбора стартового сегмента. При этом, так как параметрический множитель η_4 известен как на стороне передатчика, так и приемника, а механизм, представленный выражениями (8) и (9), устраняет неопределенность (7), то обеспечивается однозначное определение сегмента $C(a;b)$, в пределах которого далее определяются координаты стартовой точки. В свою очередь, способ выбора координат $(m;n)$ стартовой точки внутри сегмента целесообразно реализовать также с применением порогового подхода, принимая во внимание особенности его содержания. Для этого каждая из координат определяется раздельно. В этом случае координата m определяется в соответствии со следующим принципом:

1. Выполняется расчет статистических характеристик Θ_3, Θ_4 и Θ_5 сегментов $C(a;b)$ в пределах контейнера F.

2. Определяются величины $\Theta_3^{(p)}, \Theta_4^{(p)}$ и $\Theta_5^{(p)}$ аналогично способу вычисления $\Theta_2^{(p)}$ и $\Theta^{(p)}$.

3. Вычисляется битовая последовательность $B = \{b_1; b_2; b_3\}$, в которой расчет значения каждого бита выполняется на основе следующей системы выражений:

$$\begin{cases} \Theta_3 \in [\Theta_3^{(p)}; \eta_5\Theta_3^{(p)}] \to b_1 = 1; \\ \Theta_3 \in (\eta_5\Theta_3^{(p)}; 0] \to b_1 = 0; \\ \Theta_4 \in [\Theta_4^{(p)}; \eta_6\Theta_4^{(p)}] \to b_2 = 1; \\ \Theta_4 \in (\eta_6\Theta_4^{(p)}; 0] \to b_2 = 0; \\ \Theta_5 \in [\Theta_5^{(p)}; \eta_7\Theta_5^{(p)}] \to b_3 = 1; \\ \Theta_5 \in (\eta_7\Theta_5^{(p)}; 0] \to b_3 = 0, \end{cases} \tag{10}$$

где $\eta_5, \eta_6, \eta_7 < 0$ – параметрические множители, являющиеся элементами стеганографического ключа.

4. Используя элементы полученной последовательности B, координата m определяется на основе выражения, переводящего последовательность бит в десятичное число:

$$m = b_1 4 + b_2 2 + b_3 + 1\,.$$

Понятно, что в этом случае $m \in [1;8]$, что и требуется в нашем случае.

В то же время, процесс вычисления координаты n может быть реализован одним из следующих способов:

— на основе имеющегося значения координаты m путем его последующей обработки;

— аналогично вычислению m на базе численного значения некого иного массива $\{\Theta'\}$ статистической характеристик сегмента $C(a;b)$ или всего контейнера;

— с использованием ранее вычисленных значений Θ_3, Θ_4 и Θ_5 множества $\{\Theta\}$ для сегментов $C(a;b)$ в пределах контейнера F и дополнительных параметрических величин;

Рассмотрим каждый вариант построения процесса определения n.

В первом случае предполагается, что относительно рассчитанного значения выполняется преобразование вида:

$$n = \varphi(m)\,. \tag{11}$$

Такой подход является наиболее предпочтительным с точки зрения быстродействия, поскольку, в отличие от других вариантов вычисления n, не требует расчетов характеристик сегментов $C(a;b)$ в пределах всего контейнера. В свою очередь, функционал φ преобразования в выражении (11) должен отвечать следующим требованиям:

— простота реализации и низкая вычислительная нагрузка, создаваемая при вычислении;

— обеспечение дополнительного механизма защиты.

Исходя из данных требований, в рамках принятой парадигмы, предлагается значение n определять, как результат сложения m по модулю 2 с параметрической величиной η_8, т. е:

$$n = m \,\mathrm{XOR}\, \eta_8 \,.$$

В то же время для реализации процесса определения второй координаты стартовой точки без явной зависимости от полученного значения m на основе вычисленных в ходе предыдущего технологического шага значений Θ_3, Θ_4 и Θ_5 предлагается рассмотреть следующий метод. В рамках данного подхода, помимо имеющихся значений статистических характеристик, используются принципы, которые представлены выражениями (10) и (). При этом формируется новая последовательность $B = \{b'_1; b'_2; b'_3\}$ бит, однако подлежит изменению логика ее построения. Для этого используется следующая система соотношений:

$$\begin{cases} \Theta_3 \in [\Theta_3^{(p)}; \eta_5\Theta_3^{(p)}] \to b'_1 = 1; \\ \Theta_3 \in (\eta_5\Theta_3^{(p)}; \eta_9\eta_5\Theta_3^{(p)}] \to b'_1 = 0; \\ \Theta_3 \in [\eta_9\eta_5\Theta_3^{(p)}; 0] \to b'_2 = 1; \\ \Theta_4 \in [\Theta_4^{(p)}; \eta_6\Theta_4^{(p)}] \to b'_2 = 0; \\ \Theta_4 \in (\eta_6\Theta_4^{(p)}; \eta_9\eta_6\Theta_4^{(p)}] \to b'_3 = 1; \\ \Theta_4 \in [\eta_9\eta_6\Theta_4^{(p)}; 0] \to b'_2 = 0, \end{cases} \tag{12}$$

где $\eta_9 < 0$ – дополнительный параметрический множитель.

Таким образом, система выражений (12) реализует механизм определения значений бит, из которых формируется B', исходя из принадлежности величин статистических характеристик Θ_3 и Θ_4 одному из трех участков пространства возможных значений. Это достигается за счет введения дополнительного множителя η_9. При этом на трех таких участках могут определяться значения не для одного, как было при формировании множества B, а сразу для двух бит. Следовательно, формируются условия для устранения явной зависимости между ранее выявленным m и значением второй искомой координаты n. С другой стороны, в этом случае не требуется дополнительных ресурсоемких вычислений. Значение координаты n, аналогично первой координате, определяется следующим образом:

$$n = b'_1 4 + b'_2 2 + b'_3 + 1 \,. \tag{13}$$

Далее, также рассмотрим случай, когда координата n определяется на основе численных значений прочих статистической характеристик сегментов $C(a;b)$, которые ранее не были получены. Понятно, что их вычисление в случае высокой разрешающей способности контейнера будет негативно влиять на скорость выполнения всего комплекса операций. Тогда, с целью минимизации вычислительных затрат, дополнительные характеристики сегментов предлагается извлекать на уровне одного из разрядов λ их битового представления. Тогда вычисление характеристик будет сведено к операциям над битами $b_{m,n}^{(\lambda)}$, что, в общем случае, можно представить в виде следующей функциональной зависимости:

$$n = \varphi\{b_{m,n}^{(\lambda)}\}, \tag{14}$$

где $b_{m,n}^{(\lambda)}$ – бит с координатами $(m;n)$ в контейнере на уровне разряда λ двоичного описания компоненты $c(m;n)^{(a,b)}$

В свою очередь, система статистических характеристик контейнера является одним из ключевых компонент рассматриваемого метода. В связи с этим требуется разработать требования к таким характеристикам, на основании чего далее предложить определенный их набор, который отвечает сформулированным требованиям.

6. Выбор и вычисление характеристик сегментов. Статистические характеристики сегментов контейнера, способы их получения и интерпретации должны удовлетворять ряду требований, а именно [8]:

— малые вычислительные затраты, что актуально для возможности обработки массивов контейнеров большой разрешающей способности в реальном времени;

— характеристики не должна быть тривиальными, что минимизирует вероятность подбора механизмов их вычисления злоумышленником;

— характеристики должны учитывать статистические и структурные особенности.

Для удовлетворения требований нетривиальности, а также учета структурно-статистических особенностей сегмента $C(a;b)$ и минимизации вычислительной нагрузки в ходе реализации данного процесса, предлагается:

— при разработке характеристик избегать использования таких, которые требуют сложных математических расчетов;

— проводить вычисление характеристик на основе простых алгоритмов;

— вычислять характеристики как на уровне компонентного, так и на уровне битового описания сегментов;

— использовать параметрические множители.

В нашем случае требуется разработать механизмы расчета статистических характеристик $\Theta_1 - \Theta_5$. Соответственно, здесь используются параметрические величины из множества $\{\mu\}$. Тогда, например, в качестве характеристики Θ_1 предлагается использовать модуль разности суммарного количество значимых и нулевых компонент $c(m;n)^{(a,b)}$, выявленных в пределах сегмента, что эквивалентно выражению:

$$\Theta_1 = \mu_1 | \sum (c(m;n)^{(a,b)} | c(m;n)^{(a,b)} \neq 0) - \sum (c(m;n)^{(a,b)} | c(m;n)^{(a,b)} = 0) | .$$

Соответственно, для вычисления Θ_2 выражение (19) может быть модифицировано к виду:

$$\Theta_2 = \mu_2 (\sum (c(m;n)^{(a,b)} | c(m;n)^{(a,b)} \neq 0) + \sum (c(m;n)^{(a,b)} | c(m;n)^{(a,b)} = 0)) .$$

В этом случае могут быть использованы значения сумм значимых и нулевых компонент, рассчитанные на предыдущем шаге, что создает условия для уменьшения общей вычислительной нагрузки.

В свою очередь, определение значения характеристики Θ_3 может выполняться на основе количества единичных бит, выявленных на уровне разряда λ двоичного описания сегмента $C(a;b)$, локализованных в пределах v строк, расположенных последовательно, начиная с ψ-й, т. е.:

$$\Theta_3 = \mu_3 \sum_{i=\psi}^{\psi+v} \sum_{m}^{8} b(i)_{m,n}^{(\lambda)} . \tag{15}$$

Далее, по аналогии с принципом, использованным для расчета характеристики Θ_3, для определения характеристики Θ_4 может применяться выражение (15), приведенное к следующему виду:

$$\Theta_4 = \mu_4 \sum_{i=\psi}^{\psi+v} \sum_{m}^{8} b(i)_{m,n}^{(\vartheta)} , \quad \vartheta \neq \lambda . \tag{16}$$

Здесь, на этапе расчета характеристики Θ_4, согласно формуле (16), используются результаты двоичной декомпозиции компонент сегмента $C(a;b)$, тем самым может быть уменьшен объем необходимых вычислений.

Наконец, характеристику Θ_5 можем рассчитать, изменив в выражении (13) или (14) строки на столбцы, число учитываемых столбцов, а также используя соответствующий множитель μ_5, например:

$$\Theta_5 = \mu_4 \sum_{i=\psi}^{\psi+\upsilon} \sum_{n}^{8} b(i)_{m,n}^{(\lambda)} , \quad \upsilon \neq v .$$

Таким образом, все требования к вычислению статистических характеристик сегментов выполнены.

7. Проблематика реализации способа обхода контейнера и способ ее устранения. В процессе обхода контейнера согласно принципам, приведенным выражениями (2) и (5), может возникнуть ситуация неопределенности, связанная с достижением его границы по одному из направлений. В этом случае, выполнение произвольного $(i+\xi)$-го шага алгоритма формально является невозможным, если выполняется следующее условие:

$$((K-k) < s_{(i+\xi)}) \vee ((L-\ell) < s_{(i+\xi)}) , \tag{17}$$

где $(K-k)$ и $(L-\ell)$ – доступные пространства смещения по горизонтальной и вертикальной оси соответственно.

Иначе говоря, необходимая величина смещения может превышать значение $(K-k)$ и/или $(L-\ell)$, что соответствует условной «границе» контейнера. Тогда в случае, когда величина $s_{(i+1)}$ превышает доступное пространство смещения, может быть реализован подход, в рамках которого при выполнении условий (17) предусматривается переход на соседнюю стороку/столбец с изменением направления обхода текущего шага на противоположное. Иначе говоря, новая координата $(m';n')$ компоненты для следующего шага в этом случае определяется на основе системы соотношений:

$$\begin{cases} c_{i+1}(m';n') := c_i(m-q;n+1)|((K-k) \le s_{(i+1)})\&((L-\ell) \ge s_{(i+1)}); \\ c_{i+1}(m';n') := c_i(m-q;n-1)|((K-k) \le s_{(i+1)})\&((L-\ell) \le s_{(i+1)}); \\ c_{i+1}(m';n') := c_i(m+1;n-q)|((K-k) \ge s_{(i+1)})\&((L-\ell) \ge s_{(i+1)}). \end{cases}$$

Такой подход характеризуется простотой реализации и отсутствием дополнительных вычислений, что способствует снижению общего времени работы алгоритма.

В свою очередь, разработанные алгоритмы встраивания данных, с одной стороны, ориентированы на частичное использование доступной емкости контейнера (а именно: пространства LSB), а, с другой стороны, не вносят искажений, характерных для базового алгоритма, тем самым нивелируя эффективность методов стегоанализа [9, 10].

В рамках изложенной концепции стеганографический ключ рассматривается как совокупность параметрических величин, полностью определяющих уникальный сценарий обхода пространства компонент яркости контейнера. В общем виде, ключ может быть представлен следующим образом:

$$K = (\{\eta\};\{\mu\}),$$

где $\{\eta\}$ и $\{\mu\}$ – множества параметрические величин, используемых для построения уникального сценария встраивания бит скрываемого сообщения и вычисления статистических характеристик сегментов контейнера соответственно.

8. Заключение. Сформулирована концепция модификации метода неравномерных смещений за счет:

— внедрения механизмов изменения направления обхода контейнера;

— обеспечения возможности превышения максимального шага смещения, доступного в базовом методе;

— применения разработанного алгоритма выбора стартовой точки встраивания.

При этом процедуры выбора направления обхода для каждого шага смещения, величины шага и выбора стартовой точки инкапсуляции выполняются с учетом значения статистических характеристик сегментов контейнера. Нетривиальность таких характеристик, а также использование параметрических величин, которые являются элементами стегоключа, способствует повышению защищенности стеганограмм.

Применение параметрических величин в ходе выбора шага и направления смещения и при вычислении характеристик сегментов позволяет также гибко модифицировать алгоритм. Тем самым обеспечивается возможность реализации квази-случайного сценария обхода пространства компонент яркости контейнера, учитывающего особенности содержания его сегментов.

В то же время, поскольку предложенные механизмы вычисления характеристик сегментов контейнера не требуют больших объемов сложных математических вычислений, это создает условия для возможности обработки множества контейнеров большой разрешающей способности в реальном времени.

Применение предложенных механизмов модификации метода неравномерных смещений потенциально способствует устранению недостатков, изначально присущих базовому методу. За счет этого создаются условия для увеличения защищенности стеганограмм без существенного увеличения сложности всего алгоритма.

Дальнейшее развитие изложенной концепции предполагает разработку механизма формирования стегоключа путем хеш-преобразования начальной парольной фразы, а также ее адаптацию к условиям, когда носителем скрываемых данных является динамическая видеосреда.

References

1. Fridrich Y. Steganography in Digital Media: Principles, Algorithms and Applicaticks. Cambridge, Cambridge Press; 2010, 462 p.
2. Shelukhin OI., Kanaev SD. Steganography. Algorithms and software implementation. Moscow, Hotline-Telecom, scientific and technical publishing house; 2017, 592 p.
3. Gonzalez R., Woods R. Digital image processing. Moscow, Technosphere, 2012; 110 p.

4. Kobayashi H., Kiya H. Bitstream-Based JPEG Image Encryption with File-Size Preserving. IEEE 7th Global Conference on Consumer Electronics (GCCE), NY; 2018, 1-4.
5. Miano J. Image compression formats and algorithms in action: tutorial. Moscow; 2003, 336 p.
6. Westfeld A., Pfitzmann A. Attacks on Steganographic Systems Breaking the Steganographic Utilities EzStego, Jsteg, Steganos, S-Tools and Some Lessons Learned. Proceedings of The Workshop of Information Hiding. NY. 1999;1:16.
7. Tsai Ch.-L., Chen Ch.-J., Hsu W.-L. Multi-morphological image data hiding based on the application of Rubik's cubic algorithm. IEEE International Carnahan Conference on Security Technology (ICCST). 2012;1:135–139.
8. Moulin P., O'Sullivan J. A. Information-theoretic analysis of information hiding. *IEEE International Symposium on Information Theory*. 2003;49(3):563–593.
9. Qiudong Sun, Wenxin Ma, Wenying Yan, Hong Dai. Information Hiding Method Based on Block DWT Sub-Band Feature Encoding. *Journal of Software Engineering and Applications*. 2009;2(5):256–268.
10. Yanping Zhang, Juan Jiang, Yongliang Zha, Heng Zhang, Shu Zhao. Research on Embedding Capacity and Efficiency of Information Hiding Based on Digital Images. International Journal of Intelligence Science. 2013;3(2):248–156.

Конфликт интересов: о потенциальном конфликте интересов не сообщалось.
Conflict of interest: no potential conflict of interest related to this article was reported.

Поступила в редакцию 07.10.2024
Поступила после рецензирования 20.11.2024
Принята к публикации 23.11.2024

Received October 7, 2024
Revised November 20, 2024
Accepted November 23, 2024

СВЕДЕНИЯ ОБ АВТОРАХ

Твердохлеб Виталий Викторович – кандидат технических наук, доцент, доцент кафедры программного обеспечения вычислительной техники, Белгородский государственный технологический университет им. В. Г. Шухова, г. Белгород, Россия

Хлопов Андрей Михайлович – кандидат физико-математических наук, доцент, доцент кафедры программного обеспечения вычислительной техники, Белгородский государственный технологический университет им. В. Г. Шухова, г. Белгород, Россия

Акиньшин Данил Иванович – аспирант, Белгородский государственный технологический университет им. В. Г. Шухова, г. Белгород, Россия

INFORMATION ABOUT THE AUTHORS

Vitalii V. Tverdokhleb – Candidate of Technical Sciences, Assosiate Professor, Assosiate Professor of the Department of Computer Engineering Software, Belgorod State Technological University named after V. G. Shukhov, Belgorod, Russia

Andrey M. Khlopov – Candidate of Physical and Mathematical Sciences, Assosiate Professor, Assosiate Professor of the Department of Computer Engineering Software, Belgorod State Technological University named after V. G. Shukhov, Belgorod, Russia

Danil I. Akinshin – Graduate Student, Belgorod State Technological University named after V. G. Shukhov, Belgorod, Russia

К содержанию