

МЕТОД ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ КОСВЕННОГО СТЕГАНОГРАФИЧЕСКОГО ВСТРАИВАНИЯ В АДАПТИВНОМ ПОЗИЦИОННОМ ПРОСТРАНСТВЕ

Фролов О.В., Баранник В.В., Баранник Н.В.

Введение

Глобализация в сфере информационных технологий, интенсивное развитие технологий информатизации и управления в различных сферах деятельности общества сопровождается повышением значимости информационных ресурсов. С одной стороны, использование информационных систем облегчает сбор, обработку и обмен информацией, с другой стороны наблюдается постоянное увеличение объемов информационных данных, а соответственно и развитие подходов для их защиты.

Наиболее остро стоит вопрос обеспечения защищенности государственных информационных ресурсов. Такие информационные ресурсы являются собственностью государства и требуют защиты в соответствии с законодательством. Значимость государственного информационного ресурса обусловлена наличием потенциального злоумышленника, действия которого направлены на нарушение конфиденциальности, целостности и доступности государственной информации. Потеря или подмена даже части такой информации могут привести к негативным экономическим и политическим последствиям, привести к значительным потерям материальных и человеческих ресурсов.

Наиболее распространенными на практике подходами обеспечения безопасности информации являются криптографические методы. Но в тоже время существуют некоторые ограничения при использовании криптографии для обеспечения информационной безопасности, а именно:

- повышенное внимание потенциального злоумышленника к криптографически зашифрованному сообщению;
- развитие современных математических моделей для осуществления криптографического анализа;
- использование стандартизированных и беспроводных каналов передачи государственного информационного ресурса.

Для устранения существующих ограничений при использовании криптографических методов необходимо использовать скрытую передачу данных. На сегодняшний день существует большое количество стеганографических методов, которые позволяют скрытно передавать информацию в контейнере, который не привлекает внимание [1]. Наибольший интерес представляют цифровые стеганографические методы встраивания информации в цифровые изображения. Это обусловлено рядом причин, а именно: широким распространением цифровых

изображений, большим объемом мультимедийного файла, наличием в изображениях областей с визуальной избыточностью [2].

Существующие стеганографические подходы условно можно разделить на методы косвенного и непосредственного встраивания. Непосредственное встраивание реализуется путем замены элемента изображения-контейнера на элемент скрываемого сообщения. Наоборот, в косвенных методах встраивание осуществляется на основе создания зависимости между элементами путем их модификации [3].

В сравнении с методами непосредственного встраивания, косвенные подходы имеют некоторые преимущества при обеспечении безопасности государственного информационного ресурса, а именно:

- повышенной стойкостью встроенных данных к атакам и стеганографическому анализу;
- отсутствием привязки к конкретному формату представления контейнера;
- наличием возможности использования известного на приемной стороне изображения-контейнера.

Анализ существующих методов косвенного стеганографического встраивания выявил следующие недостатки при обеспечении безопасности государственного информационного ресурса [2]:

1. Низкое значение стойкости стеганограммы к визуальным атакам злоумышленника.
- 2 Низкая устойчивость встроенных данных к активным атакам злоумышленника.
3. Неудовлетворительное значение объема встраиваемых данных.
4. Необходимость наличия на приемной стороне прототипа исходного изображения-контейнера для однозначного изъятия встроенной информации.

Существующие недостатки методов непосредственного встраивания обусловлены тем, что существующие алгоритмы используют для косвенного встраивания психовизуальную избыточность изображения.

Значит, целью *научно-прикладного исследования* является проектирование стеганографической системы на основе подхода, который учитывает не только психовизуальные закономерности в изображении, а и структурные зависимости между элементами представления изображения-контейнера.

1. Разработка подхода для проектирования метода косвенного стеганографического встраивания

При проектировании стеганографической системы для обеспечения конфиденциальности служебной информации государственных структур и ведомственных организаций предлагается использовать функционально

преобразование, которое учитывает структурные зависимости между элементами изображения-контейнера.

В качестве функционального преобразования, предлагается использовать функционал для адаптивного позиционного числа, а в качестве элемента изображения-контейнера фрагмент изображения F размерностью m строк и n столбцов.

Предложенное функциональное преобразование позволяет выявить структурные закономерности в изображении. Такие закономерности обусловлены ограничением на динамический диапазон. Величина ψ динамического диапазона представления фрагмента F изображения-контейнера определяется на основе следующего выражения:

$$\psi = \max_{1 \leq i \leq m} \{c_{i,j}\} + 1, \quad j = \overline{1, n}. \quad (1)$$

Здесь $c_{i,j}$ – j -й элемент в i -ой строке массива F .

В процессе реализации функционального преобразование на основе для адаптивного позиционного числа (АПЧ) фрагмент F исходного изображения рассматривается как множество адаптивных позиционных чисел $\{C(j)\}$:

$$C(j) = \{c_{1,j}; \dots; c_{i,j}; \dots; c_{m,j}\}.$$

Значения кода $K(j)$ будет определяться, как сумма произведений элементов позиционного числа $C(j)$ на их весовые коэффициенты $V_{i,j}$ по формуле:

$$K(j) = \sum_{i=1}^m c_{i,j} V_i. \quad (2)$$

Здесь $c_{i,j}$ – $(i; j)$ -й элемент адаптивного позиционного числа $C(j)$; V_i – весовой коэффициент элемента $a_{i,j}$ адаптивного позиционного числа $C(j)$ фрагмента F .

Весовой коэффициент $V_{i,j}$ элемента $c_{i,j}$ зависит от его позиции в числе $C(j)$ и вычисляется как сумма оснований всех младших элементов АПЧ. Но учитывая, что основания ψ для всех элементов $c_{i,j}$ позиционного числа $C(j)$ вычисляется адаптивно и принимает одинаковое значение, то весовой коэффициент $V_{i,j}$ будет вычисляться по следующей формуле:

$$V'_{i,j} = V_i = \psi^{m-i}. \quad (3)$$

Второй этап предусматривает формирование кодограммы $S(F)$, которая включает служебную составляющую $S(\Psi)$ и информационную составляющую $S(j)$. Данный этап реализуется при помощи оператора выделения разрядов $\varphi_c(\bullet)$ по формуле:

$$S(F) = \varphi_c(S(j), \Psi),$$

где Ψ - базис, содержащий информацию об основаниях для адаптивных позиционных чисел фрагмента F ;

$S(j)$ - кодограмма кодового представления адаптивного позиционного числа $C(j)$.

Кодограмма $S(j)$ имеет следующий вид:

$$S(j) = \{s_1, \dots, s_\xi, \dots, s_{q(S(j))}\},$$

где $q(S(j))$ – длина двоичной кодограммы $S(j)$;

s_ξ - ξ -й двоичный разряд кодограммы $S(j)$.

Процесс реконструкции элемента $c_{i,j}$ для адаптивного позиционного числа $C(j)$ на основе кода $K(j)$ выполняется по формуле

$$c'_{i,j} = [K(j)/V_i] - [(K(j)/(\psi V_i))] \psi,$$

или

$$c'_{i,j} = \left[\sum_{i=1}^m c_{i,j} V_i / V_i \right] - \left[\sum_{i=1}^m c_{i,j} V_i / (\psi V_i) \right] \psi.$$

Такое преобразование осуществляется без внесения искажений.

В случае адаптивного позиционного кодирования, значение реконструированного элемента $c_{i,j}$ числа $C(j)$ фрагмента F не меняется в случае кодирования и декодирования с различными основаниями ψ и ψ' , т.е.

$$\begin{aligned} c'_{i,j} = c_{i,j} &= [K(j)/V_i] - [(K(j)/(\psi V_i))] \psi = \\ &= [K'(j)/V'_i] - [(K'(j)/(\psi' V'_i))] \psi' = c''_{i,j}, \end{aligned} \quad (4)$$

где $c'_{i,j}$ - элемент числа $C(j)$, реконструированный на основе системы оснований Ψ ;

$c''_{i,j}$ - элемент числа $C(j)$, реконструированный на основе системы оснований Ψ' ;

$K(j)$ - кодовое представление числа $C(j)$, сформированное в базисе оснований Ψ ;

$K'(j)$ - кодовое представление числа $C(j)$, сформированное в базисе оснований Ψ' ;

ψ' - значение модифицированного основания элемента $c'_{i,j}$.

Докажем, что значение реконструированного элемента $c_{i,j}$ числа $C(j)$ фрагмента F не меняется в случае кодирования и декодирования с различными основаниями ψ и ψ' , при условии что:

$$\psi' \geq \psi.$$

Для этого распишем левую часть выражения (4) с учетом соотношения для кода $K(j)$:

$$K(j) = \sum_{i=1}^m c_{i,j} V_i.$$

Тогда получим:

$$c'_{i,j} = \left[\sum_{i=1}^m c_{i,j} V_i \right] / V_i - \left[\sum_{i=1}^m c_{i,j} V_i \right] / (\psi V_i) \cdot \psi. \quad (5)$$

Рассмотрим первое слагаемое выражения (5):

$$\left[\sum_{i=1}^m c_{i,j} V_i \right] / V_i = \left[\sum_{\xi=1}^i c_{\xi,j} V_\xi + \sum_{\xi=i+1}^m c_{\xi,j} V_\xi \right] / V_i.$$

Перепишем данное выражение с учетом следующего соотношения:

$$V_i > \sum_{\xi=i+1}^m c_{\xi,j} V_\xi. \quad (6)$$

В этом случае получим преобразованное значение первого слагаемого выражения (5):

$$\left[\sum_{i=1}^m c_{i,j} V_i \right] / V_i = \left[\sum_{\xi=1}^i c_{\xi,j} V_\xi \right] / V_i. \quad (7)$$

Теперь преобразуем полученное выражение с учетом формулы для весового коэффициента V_i :

$$V_i = \psi^{m-i}. \quad (8)$$

Тогда выражение (8) примет следующий вид:

$$\left[\sum_{\xi=1}^i c_{\xi,j} V_\xi \right] / V_i = \left[\sum_{\xi=1}^i c_{\xi,j} \cdot \psi^{m-\xi} \right] / \psi^{m-i} = \sum_{\xi=1}^i c_{\xi,j} \cdot \psi^{i-\xi}.$$

На следующем этапе рассмотрим второе слагаемое выражения (5):

$$\left[\sum_{i=1}^m c_{i,j} V_i' \right] / (\psi V_i') \cdot \psi.$$

Перепишем данное выражение с учетом следующего неравенства:

$$\psi V_{i,j} > \sum_{\xi=i}^m c_{i,j} V_i. \quad (9)$$

В этом случае второе слагаемое выражения (5) примет вид:

$$\left[\frac{\sum_{i=1}^m c_{i,j} V_i}{\Psi V_i} \right] = \left[\frac{\sum_{\xi=1}^{i-1} c_{\xi,j} V_{\xi} + \sum_{\xi=i}^m c_{\xi,j} V_{\xi}}{\Psi V_i} \right] = \left[\frac{\sum_{\xi=1}^{i-1} c_{\xi,j} V_{\xi}}{\Psi V_i} \right]. \quad (10)$$

Преобразуем полученное выражение (10) с учетом формулы (9):

$$\left[\frac{\sum_{\xi=1}^{i-1} c_{\xi,j} V_{\xi}}{\Psi V_i} \right] = \left[\frac{\sum_{\xi=1}^{i-1} c_{\xi,j} \cdot \Psi^{m-\xi}}{\Psi \Psi_i^{m-i}} \right] = \sum_{\xi=1}^{i-1} c_{\xi,j} \cdot \Psi^{i-\xi-1}.$$

Перепишем выражение (5) с учетом выполненных преобразований. В этом случае выражение (5) примет следующий вид:

$$\begin{aligned} c'_{i,j} &= \sum_{\xi=1}^i c_{\xi,j} \cdot \Psi^{i-\xi} - \left[\sum_{\xi=1}^{i-1} c_{\xi,j} \cdot \Psi^{i-\xi-1} \right] \cdot \Psi = \\ &= \sum_{\xi=1}^i c_{\xi,j} \cdot \Psi^{i-\xi} - \sum_{\xi=1}^{i-1} c_{\xi,j} \cdot \Psi^{i-\xi} = c_{i,j}. \end{aligned} \quad (11)$$

Теперь перепишем правую часть выражения (5) с учетом формулы для кода $K'(j)$, сформированного с учетом модифицированного основания Ψ' :

$$K'(j) = \sum_{i=1}^m c_{i,j} V'_i.$$

Тогда получим:

$$c''_{i,j} = \left[\sum_{i=1}^m c_{i,j} V'_i / V'_i \right] - \left[\sum_{i=1}^m c_{i,j} V'_i / (\Psi' V'_i) \right] \cdot \Psi'. \quad (12)$$

Рассмотрим первое слагаемое выражения (12):

$$\left[\frac{\sum_{i=1}^m c_{i,j} V'_i}{V'_i} \right] = \left[\frac{\sum_{\xi=1}^i c_{\xi,j} V'_{\xi} + \sum_{\xi=i+1}^m c_{\xi,j} V'_{\xi}}{V'_i} \right].$$

Перепишем данное выражение с учетом соотношения (6). В этом случае получим первое слагаемое выражения (12) будет иметь вид:

$$\left[\frac{\sum_{i=1}^m c_{i,j} V'_i}{V'_i} \right] = \left[\frac{\sum_{\xi=1}^i c_{\xi,j} V'_{\xi}}{V'_i} \right]. \quad (13)$$

Теперь преобразуем полученное выражение с учетом формулы (8) для весового коэффициента V'_i :

$$\left[\frac{\sum_{\xi=1}^i c_{\xi,j} V'_{\xi}}{V'_i} \right] = \left[\frac{\sum_{\xi=1}^i c_{\xi,j} \cdot \psi'^{m-\xi}}{\psi'^{m-i}} \right] = \sum_{\xi=1}^i c_{\xi,j} \cdot \psi'^{i-\xi}.$$

Теперь рассмотрим второе слагаемое выражения (12):

$$\left[\frac{\sum_{i=1}^m c_{i,j} V'_i}{\psi' V'_i} \right] \cdot \psi'.$$

Перепишем данное выражение с учетом неравенства (9). Тогда получим:

$$\left[\frac{\sum_{i=1}^m c_{i,j} V'_i}{\psi' V'_i} \right] = \left[\frac{\sum_{\xi=1}^{i-1} c_{\xi,j} V'_{\xi} + \sum_{\xi=i}^m c_{\xi,j} V'_{\xi}}{\psi' V'_i} \right] = \left[\frac{\sum_{\xi=1}^{i-1} c_{\xi,j} V'_{\xi}}{\psi' V'_i} \right]. \quad (14)$$

Преобразуем полученное выражение (14) с учетом формулы (8):

$$\left[\frac{\sum_{\xi=1}^{i-1} c_{\xi,j} V'_{\xi}}{\psi' V'_i} \right] = \left[\frac{\sum_{\xi=1}^{i-1} c_{\xi,j} \cdot \psi'^{m-\xi}}{\psi' \cdot \psi'^{m-i}} \right] = \sum_{\xi=1}^{i-1} c_{\xi,j} \cdot \psi'^{i-\xi-1}.$$

Перепишем выражение (12) с учетом выполненных преобразований. В этом случае выражение (12) примет следующий вид:

$$\begin{aligned} c''_{i,j} &= \sum_{\xi=1}^i c_{\xi,j} \cdot \psi'^{i-\xi} - \left[\sum_{\xi=1}^{i-1} c_{\xi,j} \cdot \psi'^{i-\xi-1} \right] \cdot \psi' = \\ &= \sum_{\xi=1}^i c_{\xi,j} \cdot \psi'^{i-\xi} - \sum_{\xi=1}^{i-1} c_{\xi,j} \cdot \psi'^{i-\xi} = c_{i,j}. \end{aligned}$$

Теперь перепишем выражение (4) с учетом преобразованной правой и левой части:

$$c'_{i,j} = c''_{i,j} = c_{i,j}.$$

Откуда можно заключить, что значения реконструированных элементов $c_{i,j}$ числа $S(j)$ фрагмента F не меняется в случае кодирования и декодирования с различными основаниями ψ и ψ' . Графически это можно представить, как показано на рис. 1.

Значит, значения реконструируемого элемента $c_{i,j}$ в числе $S(j)$ не меняется в случае кодирования и декодирования с различными основаниями ψ и ψ' .

Предлагается использовать свойство однозначности декодирования адаптивных позиционных чисел при создании метода косвенного стеганографического встраивания служебной информации.

При проектировании метода стеганографического встраивания необходимо разработать подход модификации оснований адаптивных позиционных чисел для косвенного встраивания служебной информации.

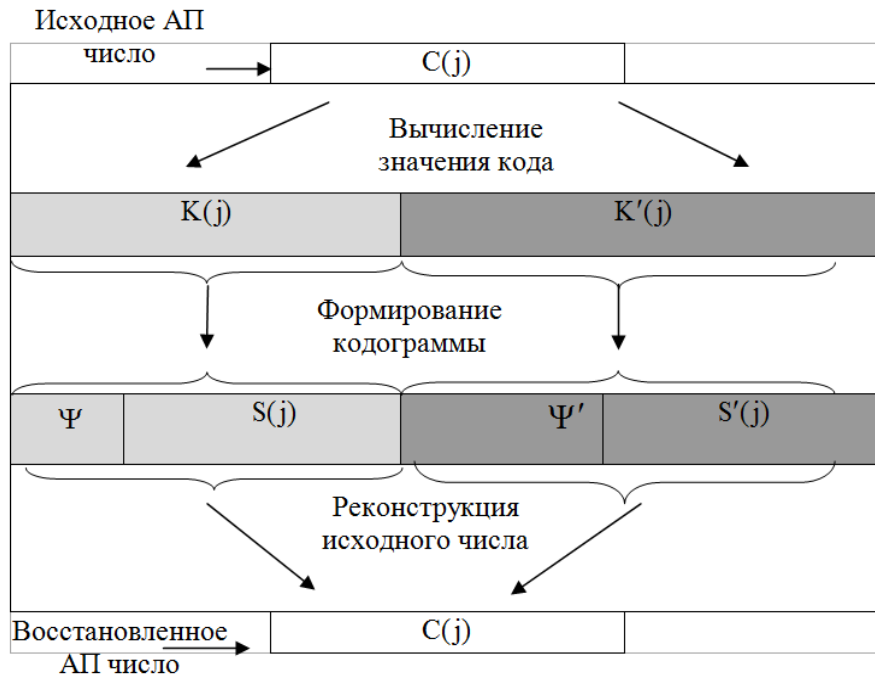


Рис. 1. Графическая интерпретация свойства адаптивного позиционного кодирования

2. Создание метода адаптивного косвенного стеганографического встраивания служебной информации на основе использования функционала для адаптивного позиционного числа

Для обеспечения конфиденциальности служебной информации косвенное встраивание элемента b_ξ скрываемого сообщения $B = \{b_1; \dots; b_\xi; \dots; b_v\}$ предлагается проводить в блок изображения-контейнера путем модификации основания ψ_i базиса Ψ на основе следующего правила:

$$\psi' = \psi + k, \text{ где } k = b_\xi.$$

Здесь ψ' - основание, модифицированное в результате косвенного стеганографического встраивания; k - коэффициент модификации.

На следующем этапе вычисляется значение кода $K'(j)$ для числа $C(j)$ с учетом модифицированного основания ψ' :

$$K'(j) = \sum_{i=1}^m c_{i,j} \psi'.$$

Третий этап предусматривает формирование кодограммы $S'(F)$, которая включает служебную составляющую $S(\Psi')$ и информационную составляющую $S'(j)$:

$$S'(F) = \varphi_c(S'(j), \Psi'),$$

где φ_c - оператор выделения разрядов.

Встраивание элементов скрываемого сообщения предлагается осуществлять в двоичном виде $b_\xi \in [0; 1]$. В этом случае встраивание будет вносить минимальные искажения. Тогда, коэффициент k модификации предлагается выбрать на основе следующего правила:

$$k = \begin{cases} 0, & b_\xi \rightarrow = 0; \\ 1, & b_\xi \rightarrow = 1. \end{cases}$$

В этом случае косвенное встраивание бита $b_\xi \in [0; 1]$ будет выполняться по формуле:

$$\Psi' = \begin{cases} \max_{1 \leq j \leq n} \{c_{i,j}\} + 1, & b_\xi \rightarrow = 0; \\ \max_{1 \leq j \leq n} \{c_{i,j}\} + 1 + 1, & b_\xi \rightarrow = 1. \end{cases} \quad (15)$$

Перепишем выражение (15) с учетом формулы (1). Тогда получим:

$$\Psi' = \begin{cases} \Psi, & b_\xi \rightarrow = 0; \\ \Psi + 1, & b_\xi \rightarrow = 1. \end{cases} \quad (16)$$

или

$$\Psi' = \Psi + b_\xi. \quad (17)$$

Таким образом, предложенный подход позволяет осуществить косвенное стеганографическое встраивание сообщения $V = \{b_1; \dots; b_\xi; \dots; b_v\}$, $b_\xi \in [0; 1]$, $\xi = \overline{1, v}$ в блоки исходного изображения-контейнера.

Теперь рассмотрим этапы функционирования стеганографической системы, построенной на основе разработанного метода косвенного встраивания. Данная система позволяет встроить бит скрываемого сообщения путем модификации основания адаптивного позиционного числа. Обратное стеганографическое преобразование осуществляется по биполярному принципу для авторизованного и неавторизованного пользователя.

Стеганографическая система включает в себя следующие базовые составляющие:

I. Косвенное стеганографическое встраивание.

Косвенное стеганографическое встраивание схематично представлено на рис. 2 и включает следующие действия:

1. Выявление основания в выбранном блоке $F_{\tau, \gamma}$. Данный этап реализуется на основе следующего выражения:

$$\Psi = \max_{1 \leq i \leq m} \{c_{i,j}\} + 1, \quad j = \overline{1, n}.$$

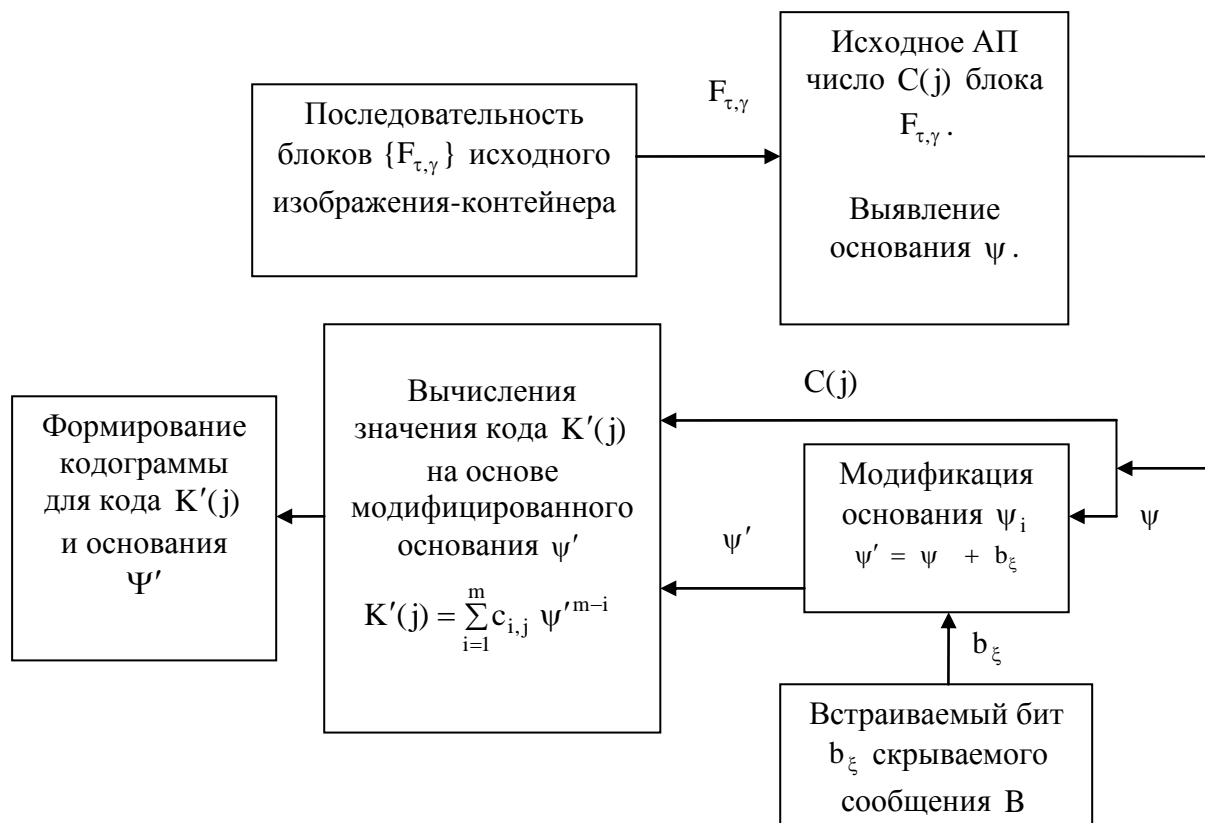


Рис. 2. Схема косвенного стеганографического встраивания

2. Косвенное встраивание бита b_ξ скрываемого сообщения $B = \{b_1; \dots; b_\xi; \dots; b_v\}$, $\xi = \overline{1, v}$ путем модификации основания ψ по следующему правилу:

$$\psi' = \begin{cases} \psi, & b_\xi \rightarrow = 0; \\ \psi + 1, & b_\xi \rightarrow = 1. \end{cases}$$

3. Формирование кода $K'(j)$ для адаптивного позиционного числа $C(j)$ блока $F_{\tau,\gamma}$. Вычисление кода $K'(j)$ выполняется с учетом модифицированного основания ψ' по формуле:

$$K'(j) = \sum_{i=1}^m c_{i,j} \psi'^{m-i}.$$

4. Формирование кодограммы, которая содержит служебную $S(\Psi')$ (основание ψ') и информационную $S(j)$ составляющую.

II. Теперь рассмотрим процесс извлечения встроенных данных.

Данный этап осуществляется при авторизованном доступе. При этом авторизованному пользователю известно ключевая информация, которая представляет собой ключевое правило встраивания. Обратное стеганографическое преобразование подразумевает проведение оценки области встраивания на основе ключевого правила.

Схема косвенного стеганографического изъятия представлена на рис. 3 и включает следующие этапы:

1. Извлечение из кодограммы кода $K'(j)$ при помощи основания ψ' .
2. Восстановление элементов исходного числа:

$$c'_{i,j} = [K'(j)/V'_i] - [K'(j)/(\psi' V'_i)] \psi'$$

3. Выявление исходного основания ψ по формуле:

$$\psi'' = \max_{1 \leq i \leq m} \{c'_{i,j}\} + 1, \quad j = \overline{1, n}. \quad (18)$$

где ψ''_i - i -й основание восстановленного базиса Ψ'' .

4. Косвенное изъятие встроенного бита b'_ξ . Данный этап реализуется на основе сравнения модифицированного ψ' и восстановленного ψ''

основания на основе следующего выражения:

$$b'_\xi = \begin{cases} 0, & \rightarrow \psi' - \psi'' = 0; \\ 1, & \rightarrow \psi' - \psi'' = 1. \end{cases}$$

или

$$b'_\xi = \psi' - \psi'' . \quad (19)$$

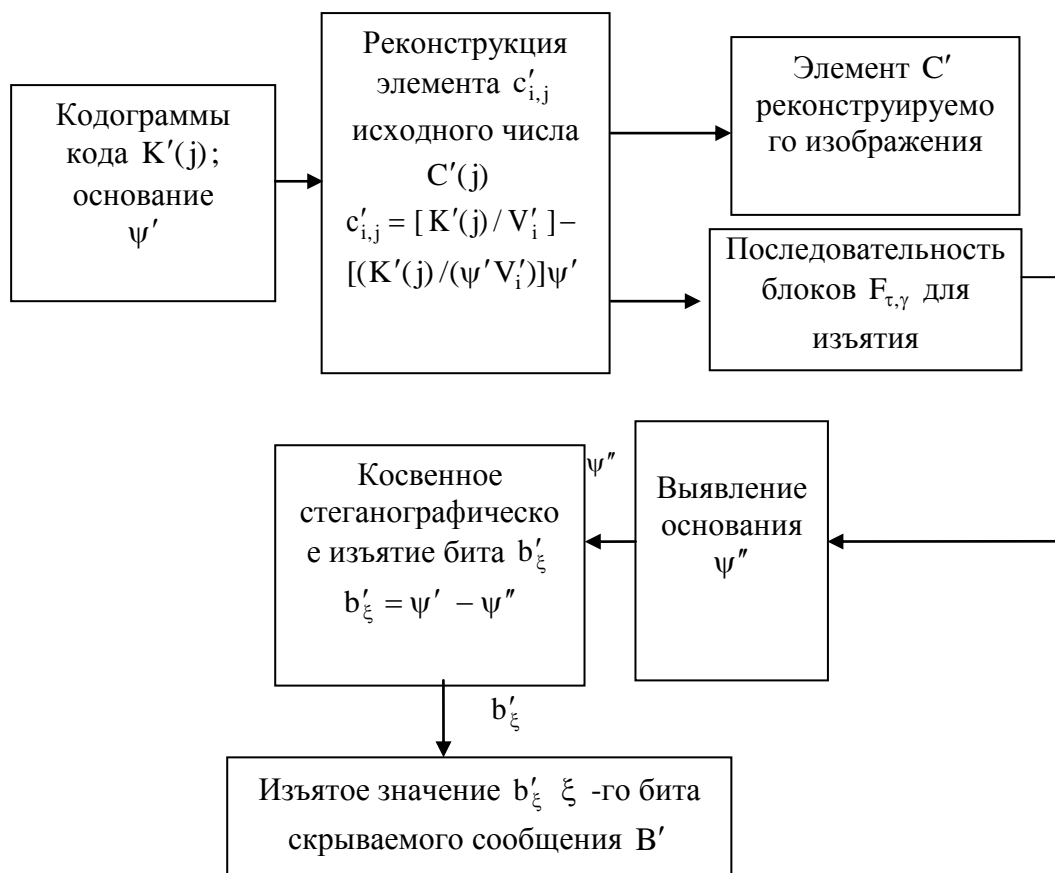


Рис 3. Схема косвенного стеганографического изъятия.

Докажем, что разработанная стеганографическая система позволяет осуществить безошибочное изъятие встроенного бита b'_ξ , т.е.

$$b'_\xi = b_\xi. \quad (20)$$

В этом случае, учитывая выражения (17) и (19) также должно выполняться следующее условие:

$$\psi' - \psi'' = \psi' - \psi. \quad (21)$$

Тогда при отсутствии активных и пассивных воздействий на кодовое представление числа, значения исходных и принятых модифицированных оснований равны. Отсюда, безошибочное изъятие будет осуществляться при выполнении следующего условия:

$$\psi'' = \psi.$$

Учитывая, что значения оснований ψ' и ψ определяются на основе выражений соответственно (1) и (18), то для доказательства условия (21) необходимо выполнение следующего равенства:

$$c'_{i,j} = c_{i,j}.$$

Доказательство выполнения данного равенства приведено в выражениях (8-14). Отсюда следует, что стеганографическая система косвенного встраивания позволяет изъять 100% встроенной информации.

Теперь рассмотрим обратное стеганографическое преобразование в случае неавторизованного доступа. В этом случае у злоумышленника отсутствует ключевое правило встраивания, а декодирование будет содержать следующие действия:

1. Извлечение из кодограммы кода $K'(j)$ при помощи основания ψ' .
2. Восстановление элементов исходного числа:

$$c''_{i,j} = [K'(j)/V'_i] - [K'(j)/(\psi' V'_i)] \psi'.$$

где $c''_{i,j}$ - i -й элемент реконструируемого числа $C''(j)$, как составляющей реконструируемого фрагмента F при неавторизованном доступе.

Выводы

1. Разработан подход для осуществления косвенного стеганографического встраивания служебной информации на основе использования прямого и обратного функционального преобразования для адаптивных позиционных чисел. Обосновано свойство однозначного обратного декодирования элементов числа при формировании кодограммы на основе исходных и модифицированных служебных данных.

Научная новизна. Впервые разработан подход для осуществления косвенного стеганографического встраивания скрываемого элемента путем модификации основания для адаптивных позиционных чисел фрагмента изображения-контейнера. В отличие от других стеганографических методов, встраивание осуществляется без модификации самих элементов

изображения, что позволяет устранить внесение визуальных искажений. Это позволяет повысить устойчивость встроенных данных к визуальным атакам злоумышленника.

2. Разработан метод косвенного стеганографического встраивания встроенных данных на основе модификации служебных данных. Для минимизации вносимых искажений предложено встраивать один бит скрываемой информации путем модификации основания адаптивного позиционного числа.

Научная новизна. Впервые разработан метод косвенного стеганографического встраивания бита скрываемого сообщения путем модификации основания фрагмента изображения-контейнера. В отличие от других методов косвенное встраивание осуществляется путем модификации оснований элементов фрагмента изображения с последующим формированием на основе модифицированного основания кодовых конструкций для адаптивных позиционных чисел. Это позволяет повысить конфиденциальность встраиваемых служебных данных в интересах государственных структур и ведомственных организаций.

3. Разработан метод косвенного стеганографического изъятия встроенного бита скрываемого сообщения на основе сравнения исходных и модифицированных оснований. Механизм обратного стеганографического изъятия предусматривает:

1) восстановление элементов исходного фрагмента изображения-контейнера на основе системы модифицированных оснований;

2) выявление системы исходных оснований из фрагмента изображения контейнера;

3) косвенное изъятие бита скрываемого сообщения путем сравнения исходных и модифицированных оснований.

Научная новизна. Впервые разработан метод обратного косвенного стеганографического преобразования на основе сравнения исходных и модифицированных оснований. В отличие от других систем, восстановление исходного фрагмента изображения-контейнера осуществляется для неавторизованного и авторизованного пользователя при наличии ключевой информации. Это позволяет скрытно встраивать бит скрываемой служебной информации в фрагмент изображения-контейнера на основе модификации служебных данных.

Литература

1. Грибунин В.Г., Оков И.Н., Туринцев И.В., Цифровая стеганография. – М.: Солон-Пресс, 2002. – 272 с.

2. Конахович Г.Ф., Пузыренко А.Ю., Компьютерная стеганография. Теория и практика. – К.: «МК-Пресс» 2006. – 288с.

3. Тарасов Д.О., Мельник А.С., Голобородько М.М. Класифікація та аналіз безкоштовних програмних засобів стеганографії // Інформаційні системи та мережі. Вісник НУ «Львівська політехніка» № 673. – Львів 2010. – С. 365 - 374.