УДК 629.391

А.К. ЮДИН, В.В. БАРАННИК, О.В. ФРОЛОВ

МЕТОД КОСВЕННОГО СТЕГАНОГРАФИЧЕСКОГО ВСТРАИВАНИЯ НА ОСНОВЕ ФУНКЦИОАНАЛЬНОГО ПРЕОБРАЗОВАНИЯ ДЛЯ АДАПТИВНОГО ПОЗИЦИОННОГО ЧИСЛА

Предлагается подход для проектирования стеганографической системы косвенного встраивания. Формулируются требования для функционального преобразования элементов изображения при стеганографическом встраивании. Приводятся свойства функционального преобразования для адаптивного позиционного числа. Разрабатывается метод косвенного стеганографического встраивания на основе использования функционального преобразования для адаптивного представления элементов изображения-контейнера. На основе метода проектируется стеганографическая система косвенного встраивания. На примере показывается процесс встраивания и извлечения встроенной информации и реконструкцией элементов изображения-контейнера.

1. Введение

Для повышения безопасности информационных ресурсов при передаче в инфокоммуникационных системах используются методы стеганографического встраивания информации в изображение.

В отличие от методов криптографической защиты стеганографические алгоритмы позволяют избежать прямых атак на скрываемое сообщение. Современные методы компьютерной стеганографии на базе изображения-контейнера условно разделены на алгоритмы:

– непосредственного стеганографического встраивания;

– косвенного стеганографического встраивания.

В сравнении с методами непосредственного встраивания методы косвенного встраивания обладают повышенной стойкостью встроенных данных в условиях применения злоумышленником активных воздействий (атак). Однако при повышенных вычислительных возможностях и разработке новых подходов для осуществления атак существующие методы косвенного встраивания не обеспечивают в полной мере системных требований к скрытию информации.

К общим недостаткам существующих методов относится использование для стеганографического встраивания психовизуальной избыточности цифровых изображений. Как правило, атаки, направленные на разрушение встроенной информации, представляют собой методы, позволяющие устранять психовизуальную избыточность. Поэтому для повышения стойкости встроенных данных в условиях изменения злоумышленником активных атак предлагается подход, основанный на использовании функционального преобразования элементов изображения-контейнера. При этом встраивание предлагается осуществлять за счет применения структурной избыточности контейнера.

2. Концепция функционального преобразования для косвенного стеганографического встраивания

Для реализации функционального преобразования элементов предлагается синтезировать функционал, который должен обеспечить следующие требования:

1. Функциональное преобразование должно обеспечивать взаимооднозначное кодирование $f(\bullet)$ и декодирование $f^{-1}(\bullet)$ массива A изображения-контейнера при наличии служебной информации Ψ, т.е. $S = f(C, \Psi)$, $C' = f^{-1}(S, \Psi)$ и $C' = C$.

Здесь C' – массив, восстановленный в результате обратного функционального преобразования $f^{-1}(S)$; Ψ – служебная информация; S – массив, полученный при выполнении прямого функционального преобразования.

2. В результате функционального преобразования массива C должна формироваться кодограмма S, которая состоит из двух частей:

– служебной, содержащей служебные данные Ψ;

– информационной , содержащей кодовое представление массива A.

3. Значения реконструированных массивов C' и C'' не должны меняться в случае формирования кода при различных значениях служебной информации (Ψ и Ψ'), т.е.

$$C' = f^{-1}(S, \Psi) = f^{-1}(S', \Psi') = C'',$$

где C' – массив, реконструированный на основе кода, сформированного с учетом служебных данных Ψ; C'' – массив, реконструированный на основе кода, сформированного с учетом модифицированных служебных данных Ψ'; S – кодограмма, полученная с учетом служебных данных Ψ; S' – кодограмма, полученная с учетом служебных данных Ψ'.

Предлагается использовать это свойство для косвенного стеганографического встраивания. Тогда процесс встраивания будет включать намеренное изменение служебной информации Ψ на основе ключевого условия. Сформированная кодограмма S', содержащая модифицированные служебные данные Ψ', передается по каналу. При этом на приемной стороне авторизированному пользователю известно условие косвенного встраивания, т.е. механизма модификации исходной служебной информации Ψ. В этом случае процесс стеганографического изъятия будет осуществляться путем анализа значений исходной Ψ и измененной Ψ' служебной информации.

Тогда прямое косвенное стеганографическое преобразование будет включать следующие этапы:

1. Формирование вектора служебных данных Ψ для массива $C''(2)$ изображения контейнера.

2. Модификацию вектора служебных данных Ψ с учетом встраиваемого элемента b_ξ на основе ключевого условия: $\Psi' = \Psi + b_\xi$. Здесь b_ξ – элемент скрываемого сообщения $B = \{b_1; ...; b_\xi; ...; b_v\}$, $\xi = \overline{1, v}$.

3. Функциональное преобразование массива C с учетом модифицированного вектора служебных данных Ψ' по правилу $f(C)$, т.е. $S = f(C, \Psi')$, где S – сформированное значение кодограммы.

Полученная кодограмма, содержащая в себе информационную составляющую S и служебную составляющую Ψ', передается в канал передачи данных, где может подвергаться атакующим воздействиям.

Обратное косвенное стеганографическое преобразование осуществляется по биполярному принципу для авторизированного и неавторизированного пользователя.

При неавторизированном доступе, по правилу $f^{(-1)}(\bullet)$ осуществляется реконструкция исходного массива изображения-контейнера: $C'' = f^{(-1)}(S; \Psi')$. Здесь C'' – массив исходного изображения, полученный в результате неавторизированного доступа.

Наоборот, обратное косвенное стеганографическое преобразование для авторизованного пользователя осуществляется с учетом ключевого условия изъятия и содержит следующие этапы:

1. На первом этапе по правилу $f^{(-1)}(\bullet)$ реконструируется массив C' исходного изображения контейнера: $C' = f^{(-1)}(S; \Psi')$. Здесь S – принятая кодограмма, сформированная на передающей стороне с учетом модифицированных служебных данных Ψ'.

2. На втором этапе для реконструированного массива C' по ключевому правилу формируется исходный вектор служебных данных Ψ.

3. Третий этап включает косвенное изъятие встроенного элемента b'_ξ скрываемого сообщения $B' = \{b'_1; ...; b'_\xi; ...; b'_v\}$ на основе ключевого условия изъятия при анализе восстановленного Ψ и полученного Ψ' векторов служебных данных: $b'_\xi = \Psi' - \Psi$.

3. Метод косвенного стеганографического встраивания на основе использования функционального преобразования для адаптивного позиционного числа

В качестве такого функционального преобразования предлагается использовать кодообразующую функцию для адаптивного позиционного числа, а в качестве элемента изображения-контейнера – фрагмент изображения F, размерность m строк и n столбцов.

Данное 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:

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

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

В процессе реализации функционального преобразования на основе адаптивного позиционного кодирования фрагмент F исходного изображения рассматривается как множество адаптивных позиционных чисел $\{C(j)\}$: $C(j) = \{c_{1,j};...; c_{i,j};...;c_{m,j}\}$.

Значения кода $K(j)$ будет определяться как сумма произведений элементов позиционного числа $C(j)$ на их весовые коэффициенты $V_{i,j}$ по формуле: $K(j) = \sum_{i=1}^{m} c_{i,j} V_i$. Здесь $c_{i,j}$ – $(i; j)$-й элемент адаптивного позиционного числа $C(j)$; V_i – весовой коэффициент элемента $c_{i,j}$ адаптивного позиционного числа $C(j)$ фрагмента F.

Весовой коэффициент V_i элемента $c_{i,j}$ зависит от его позиции в числе $C(j)$ и вычисляется как произведение оснований всех младших элементов. Весовой коэффициент V_i вычисляется по следующей формуле: $V_i = \prod_{\xi=1+1}^{m} \psi_\xi$.

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:

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

здесь $q(S(j))$ – 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

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

или

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

Такое преобразование осуществляется без внесения искажений.

В случае адаптивного представления значение реконструированного элемента $c_{i,j}$ числа C(j) фрагмента F не меняется при кодировании и декодировании с различными основаниями ψ_i и ψ'_i, т.е.

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

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'_i – значение модифицированного основания элемента $c'_{i,j}$.

Графически это показано на рис .1. Предлагается использовать данное свойство для проектирования системы косвенного стеганографического встраивания. Косвенное встраивание элемента b_ξ скрываемого сообщения $B = \{b_1;...;b_\xi;...;b_v\}$ предлагается проводить в блок изображения-контейнера путем модификации основания ψ_i базиса Ψ на основе следующего правила: $\psi'_i = \psi_i + k$, где $k = b_\xi$. Здесь ψ' – основание, модифицированное в результате косвенного стеганографического встраивания; k – коэффициент модификации.

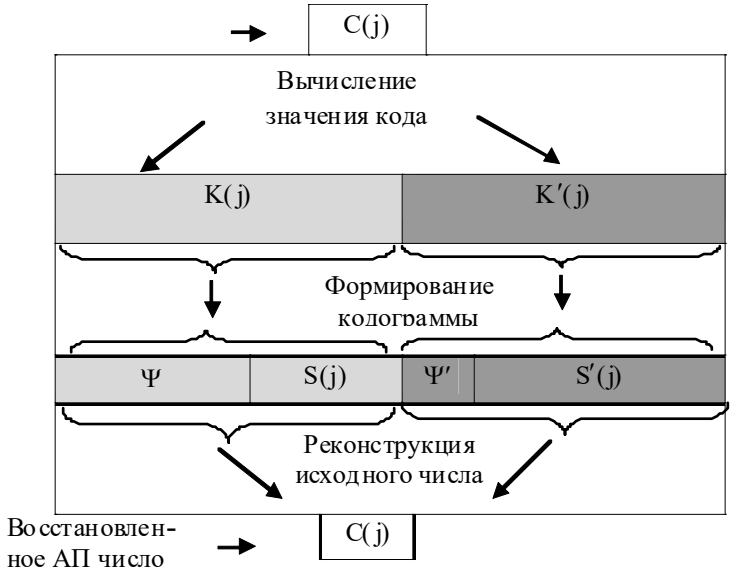

Рис. 1. Графическая интерпретация свойства адаптивного позиционного кодирования.

В процессе косвенного стеганографического встраивания необходимо учитывать потенциальную возможность увеличения длины q(S′(j)) кодограммы S′(j) относительно длины q(S(j)) исходной кодограммы. Поэтому для уменьшения уровня вносимой избыточности R встраивать элементы предлагается в двоичном представлении $b_\xi \in [0;1]$, а коэффициент k модификации выбирать на основе следующего правила:

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

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

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

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

Теперь рассмотрим этапы функционирования разработанной стеганографической системы косвенного встраивания (рис. 2).

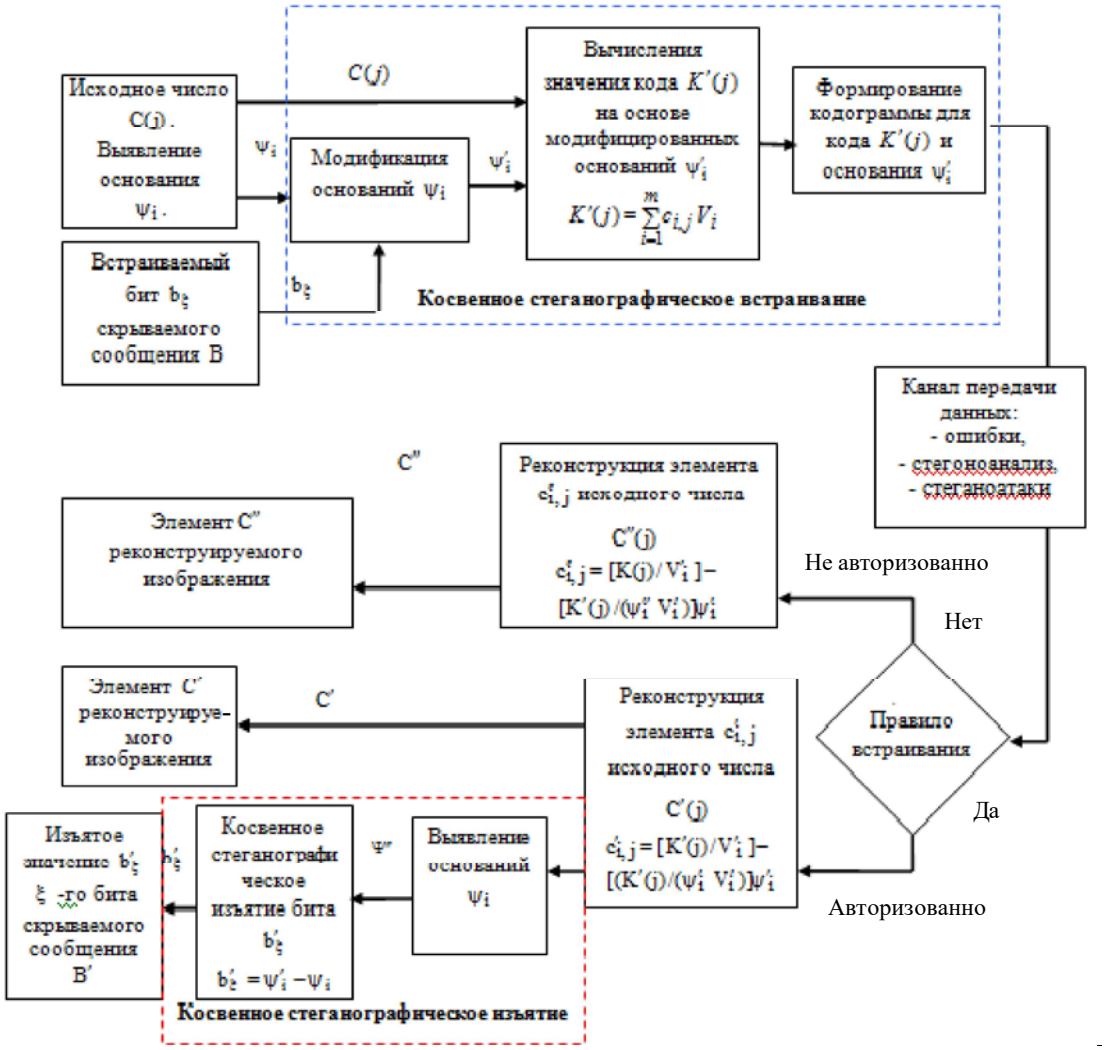

Рис. 2. Структурная схема стеганографической системы косвенного встраивания

Данная система позволяет встроить бит скрываемого сообщения путем модификации оснований адаптивного позиционного числа. Косвенное стеганографическое встраивание включает в себя следующие действия:

1. Выявление оснований в выбранном блоке $F_{\tau,\gamma}$.

Данный этап реализуется на основе следующего выражения: $\psi_i = \max\limits_{1\le i\le m}\{c_{i,j}\}+1$.

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

$$\psi'_i = \begin{cases} \psi_i\ , b_\xi \to =0; \\ \psi_i + 1,\ b_\xi \to =1. \end{cases}$$

3. Формирование кода $K'(j)$ для адаптивного позиционного числа $C(j)$ блока $F_{\tau,\gamma}$. Вычисление кода $K'(j)$ выполняется с учетом модифицированных оснований $\{\psi'_i\}$ по формуле: $K'(j) = \sum_{i=1}^{m} c_{i,j} V_i$.

4. Формирование кодограммы, которая содержит служебную $S(\Psi')$ (основания $\{\psi'_i\}$) и информационную $S(j)$ составляющую.

Схема косвенного стеганографического изъятия включает следующие этапы:

1. Извлечение из кодограммы кода $K'(j)$ при помощи оснований $\{\psi'_i\}$.

2. Восстановление элементов исходного числа: $c'_{i,j} = [K'(j)/V'_i] - [K'(j)/(\psi'_i V'_i)]\ \psi'_i$.

3. Выявление исходного основания $\{\psi_i\}$ по формуле:

$$\psi_i = \max_{1 \le i \le m} \{c_{i,j}\} + 1,$$

где ψ''_i – i-е основание восстановленного базиса Ψ''.

4. Косвенное изъятие встроенного бита b'_ξ. Данный этап реализуется на основе сравнения модифицированного ψ'_i и восстановленного ψ''_i основания на основе следующего выражения:

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

или $b'_\xi = \psi'_i - \psi''_i$.

Теперь рассмотрим обратное стеганографическое преобразование при неавторизированном доступе. В этом случае у злоумышленника отсутствует ключевое правило встраивания, а декодирование будет содержать следующие действия:

1. Извлечение из кодограммы кода $K'(j)$ при помощи оснований $\{\psi'_i\}$.

2. Восстановление элементов исходного числа: $c''_{i,j} = [K'(j)/V'_i] - [K'(j)/(\psi'_i V'_i)]\ \psi'_i$, где $c''_{i,j}$ – i-й элемент реконструируемого числа $C''(j)$ как составляющей реконструируемого фрагмента F при неавторизированном доступе.

Рассмотрим пример косвенного стеганографического встраивания бита $b_\xi = 1$ в фрагмент изображения F:

$$F = \begin{vmatrix} 2 & 2 & 3 & 1 \\ 1 & 4 & 3 & 5 \\ 4 & 1 & 4 & 2 \\ 1 & 4 & 1 & 4 \end{vmatrix}.$$

Определим основания для элементов фрагмента F: $\psi_i = \max_{1 \le i \le m} \{c_{i,j}\} + 1$.

На следующем этапе проведем косвенное встраивание бита $b_\xi = 1$ в полученный базис оснований $\psi = 5$. Для этого на основе ключевого правила вычислим модифицированное основание ψ': $\psi' = \psi + 1 = 5 + 1 = 6$.

Теперь представим фрагмент изображения F в кодовом виде с учетом модифицированного основания ψ'. В этом случае для каждого адаптивного позиционного числа $C(j)$ фрагмента F сформируем значение кода $K(j)$:

$$K(1)=\sum_{i=1}^{4} c_{i,1}\cdot V'_i = 2\cdot 216+1\cdot 36+4\cdot 6+1\cdot 1=493,$$

$$K(2)=\sum_{i=1}^{4} c_{i,2}\cdot V'_i = 2\cdot 216+4\cdot 36+1\cdot 6+4\cdot 1=448,$$

$$K(3)=\sum_{i=1}^{4} c_{i,3}\cdot V'_i = 3\cdot 216+3\cdot 36+4\cdot 6+1\cdot 1=761,$$

$$K(4)=\sum_{i=1}^{4} a_{i,4}\cdot V'_i = 1\cdot 216+5\cdot 36+2\cdot 6+4\cdot 1=412.$$

В результате косвенного стеганографического встраивания бита $b_\xi = 1$ в фрагмент изображения-контейнера была получена кодовая последовательность, представленная на рис. 3.

Рис. 3. Кодовое представление фрагмента F, полученное в результате косвенного стеганографического встраивания

Теперь рассмотрим пример косвенного стеганографического изъятия при авторизированном доступе. В этом случае пользователю известна ключевая информация, которая представляет собой правило встраивания.

На первом этапе восстановлим значения элементов $\{c'_{i,j}\}$ чисел $\{C'(j)\}$ исходного фрагмента F'. Для этого используем следующую формулу:

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

где $K'(j)$ – значение кода, считанное авторизированным пользователем.

В качестве примера осуществим восстановление числа $C'(2)$, которое соответствует второму столбцу фрагмента F' изображения-контейнера:

$$c'_{1,2} = [\ K'(2) / V'_1\ ] - [\ K'(2) / (\psi'_1\ V'_1)\ ]\ \psi'_1 =$$
$$= [\ 448/216\ ] - [\ 448/216\cdot 6\ ]\cdot 6 = 2;$$
$$c'_{2,2} = [\ K'(2) / V'_2\ ] - [\ K'(2) / (\psi'_2\ V'_2)\ ]\ \psi'_2 =$$
$$= [\ 448/36\ ] - [\ 448/36\cdot 6\ ]\cdot 6 = 4;$$
$$c'_{3,2} = [\ K'(2) / V'_3\ ] - [\ K'(2) / (\psi'_3\ V'_3)\ ]\ \psi'_3 =$$
$$= [\ 448/6\ ] - [\ 448/6\cdot 6\ ]\cdot 6 = 1;$$
$$c'_{4,2} = [\ K'(2) / V'_4\ ] - [\ K'(2) / (\psi'_4\ V'_4)\ ]\ \psi'_4 =$$
$$= [\ 448/1\ ] - [\ 448/1\cdot 6\ ]\cdot 6 = 5.$$

После декодирования восстановленный фрагмент F' изображения контейнера примет следующий вид:

$$F' = \begin{vmatrix} 2 & 2 & 3 & 1 \\ 1 & 4 & 3 & 5 \\ 4 & 1 & 4 & 2 \\ 1 & 5 & 1 & 4 \end{vmatrix}.$$

Для изъятия встроенного сообщения бита $b_\xi = 1$ авторизированному пользователю необходимо определить основание ψ'' для фрагмента F и сравнить его с основанием ψ', изъятым из служебной составляющей кодограммы. Основания ψ'' определяются по формуле $\psi''_i = \max\limits_{1 \le i \le m} \{c''_{i,j}\} + 1$. Тогда получим следующее значение исходного основания: $\psi = 5$. Теперь на основе правила $b'_\xi = \psi'_i - \psi''_i$ осуществим косвенное изъятие встроенного бита: $b'_\xi = \psi' - \psi'' = 6 - 5 = 1$,

В результате выполнения обратного стеганографического преобразования был безошибочно восстановлен встроенный бит $b_\xi = 1$.

4. Выводы

Для устранения недостатков существующих стеганографических методов косвенного встраивания предложен подход в виде применения функционального преобразования элементов изображения-контейнера. Сформулированы требования для функционального преобразования.

Разработан метод косвенного стеганографического встраивания на основе использования функционального преобразования для адаптивного позиционного числа, который базируется на следующих этапах:

– формирование основания для фрагмента изображения ;

– косвенное стеганографическое встраивание путем модификации оснований с учетом встраиваемой информации;

– формирование кодового представления элементов изображения-контейнера.

На основе сформулированного метода разработана система косвенного стеганографического встраивания скрываемой информации, которая включает следующие этапы:

1. Этап косвенного стеганографического встраивания.

2. Этап косвенного стеганографического изъятия встроенной информации.

Список литературы: 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. 288 с. **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.

Поступила в редколлегию 23.12.2015

Юдин Александр Константинович, д-р техн. наук, профессор, директор института компьютерных информационных технологий Национального авиационного университета. Адрес: Украина, 01000, Киев, пр.Космонавта Комарова, 1.

Баранник Владимир Викторович, д-р техн. наук, профессор, начальник кафедры боевого применения и эксплуатации АСУ Харьковского университета Воздушных Сил. Научные интересы: обработка и передача информации. Адрес: Украина, 61023, Харьков, ул. Сумская, 77/79.

Фролов Олег Владимирович, соискатель Национального авиационного университета. Адрес: Украина, 01000, Киев, пр.Космонавта Комарова, 1.