

МЕТОД КОСВЕННОГО СТЕГАНОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ ФУНКЦИОНАЛА ДЛЯ АДАПТИВНОГО ПОЗИЦИОННОГО КОДИРОВАНИЯ

Разрабатывается метод косвенного стеганографического встраивания на основе использования функционала для адаптивного позиционного кодирования. Проектируется система косвенного стеганографического встраивания, которая позволяет встраивать информацию путем модификации оснований элементов изображения-контейнера. Проводится анализ изображений, полученных в результате обратного стеганографического преобразования.

1. Введение

Современное развитие инфокоммуникационных сетей диктует новые требования к безопасности информационных ресурсов. Актуальным направлением для решения проблемы повышения безопасности является применение методов стеганографического встраивания.

Существующие методы стеганографии представлены алгоритмами непосредственного и косвенного встраивания. Такие методы позволяют скрытно передавать информацию с помощью психовизуальной избыточности изображения-контейнера. Недостатком указанного подхода является низкая устойчивость встроенных данных к активным воздействиям злоумышленника, направленным на разрушение встроенного сообщения. Также для таких методов характерно ухудшение визуальной устойчивости стеганограммы при попытке увеличения объема встраиваемой информации.

Возможным решением проблемы улучшения показателей визуальной устойчивости стеганограммы, а также стойкости к трансформации и атакам является использование для косвенного встраивания неравновесного позиционного кодирования. Отсюда, цель исследования состоит в разработке метода косвенного стеганографического встраивания и построении структурной модели стеганографической системы.

2. Разработка метода косвенного стеганографического встраивания на основе функционального преобразования для неравновесного позиционного кодирования

Функциональное преобразование для адаптивного позиционного кодирования 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:

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

здесь $a_{i,j}$ – 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 $\{A(j)\} : A(j) = \{a_{1,j}; \dots; a_{i,j}; \dots; a_{m,j}\}$.

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

$$N(j) = \sum_{i=1}^m a_{i,j} V_{i,j}. \quad (2)$$

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

Весовой коэффициент $V_{i,j}$ элемента $a_{i,j}$ зависит от его позиции в числе $A(j)$ и вычисляется как произведение оснований всех младших элементов. Но учитывая, что основание ψ для всех элементов $a_{i,j}$ позиционного числа $A(j)$ принимает одинаковое значение, весовой коэффициент будет $V_{i,j}$ вычисляться по следующей формуле:

$$V_i = \psi^{m-i}. \quad (3)$$

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

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

где Ψ – базис, содержащий информацию об основаниях для адаптивных позиционных чисел фрагмента F ; $C(j)$ – кодограмма кодового представления адаптивного позиционного числа $A(j)$.

Кодограмма $C(j)$ имеет следующий вид: $C(j) = \{c_1, \dots, c_\xi, \dots, c_{q(C(j))}\}$, где $q(C(j))$ – длина двоичной кодограммы $C(j)$; c_ξ – ξ -й двоичный разряд кодограммы $C(j)$.

Процесс реконструкции элемента $a_{i,j}$ для адаптивного позиционного числа $A(j)$ на основе кода $N(j)$ выполняется по формуле

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

Такое преобразование осуществляется без внесения искажений.

В случае адаптивного позиционного кодирования значение реконструированного элемента $a_{i,j}$ числа $A(j)$ фрагмента F не меняется при кодировании и декодировании с различными основаниями ψ и ψ' , т.е.

$$a'_{i,j} = a_{i,j} = \left[N(j) / V_i \right] - \left[(N(j) / (\psi V_i)) \right] \psi = \left[N'(j) / V'_i \right] - \left[(N'(j) / (\psi' V'_i)) \right] \psi' = a''_{i,j}, \quad (4)$$

где $a'_{i,j}$ – элемент числа $A(j)$, реконструированный на основе системы оснований ψ ; $a''_{i,j}$ – элемент числа $A(j)$, реконструированный на основе системы оснований ψ' ; $N(j)$ – кодовое представление числа $A(j)$, сформированное в базисе оснований ψ ; $N'(j)$ – кодовое представление числа $A(j)$, сформированное в базисе оснований ψ' ; ψ' – значение модифицированного основания элемента $a'_{i,j}$.

Докажем данное свойство адаптивного позиционного представления при условии, что $\psi' \geq \psi$. Распишем левую часть выражения (4) с учетом соотношения для кода $N(j)$:

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

Тогда получим:

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

Рассмотрим первое слагаемое выражения (5):

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

Перепишем данное выражение с учетом следующего соотношения:

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

В этом случае получим:

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

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

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

Тогда (7) примет следующий вид:

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

Теперь рассмотрим второе слагаемое выражения (5): $\left[\frac{\sum_{i=1}^m a_{i,j} V_i'}{\psi' V_i'} \right] \cdot \psi'$.

Перепишем его с учетом следующего неравенства:

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

И тогда получим:

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

Преобразуем полученное выражение с учетом формулы (8):

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

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

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

Теперь перепишем правую часть выражения (4) с учетом формулы для кода $N'(j)$, сформированного с учетом модифицированного основания ψ' : $N'(j) = \sum_{i=1}^m a_{i,j} V_i'$.

Тогда получим:

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

Рассмотрим первое слагаемое выражения (12):

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

Перепишем данное выражение с учетом соотношения (6). В этом случае получим:

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

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

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

Далее рассмотрим второе слагаемое выражения (12): $\left[\frac{\sum_{i=1}^m a_{i,j} V'_i}{\psi' V'_i} \right] \cdot \psi'$

Перепишем его с учетом неравенства (9). Тогда получим:

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

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

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

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

$$a''_{i,j} = \sum_{\xi=1}^i a_{\xi,j} \cdot \psi'^{i-\xi} - \left[\sum_{\xi=1}^{i-1} a_{\xi,j} \cdot \psi'^{i-\xi-1} \right] \cdot \psi' = \sum_{\xi=1}^i a_{\xi,j} \cdot \psi'^{i-\xi} - \sum_{\xi=1}^{i-1} a_{\xi,j} \cdot \psi'^{i-\xi} = a_{i,j}.$$

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

$$a'_{i,j} = a''_{i,j} = a_{i,j}.$$

Отсюда можно заключить, что свойство (4) доказано.

Предлагается использовать данное свойство для проектирования системы косвенного стеганографического встраивания. Косвенное встраивание элемента b_ξ скрываемого сообщения $V = \{b_1; \dots; b_\xi; \dots; b_v\}$ 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 $N'(j)$ для числа $A(j)$ с учетом модифицированного основания Ψ' : $N'(j) = \sum_{i=1}^m a_{i,j} \Psi'$.

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

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

где φ_c – оператор выделения разрядов.

Косвенное встраивание бита $b_\xi \in [0; 1]$ будет выполняться по формуле:

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

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.

3. Выводы

Разработан подход для улучшения характеристик косвенного стеганографического встраивания, включающий в себя прямое и обратное стеганографическое преобразование при помощи кодообразующего функционала для адаптивного позиционного кодирования. Косвенное встраивание предлагается проводить путем модификации оснований для блоков изображения-контейнера.

Разработана схема системы косвенного стеганографического встраивания. Система включает в себя следующие базовые составляющие:

- косвенное стеганографическое встраивание;
- косвенное стеганографическое изъятие при наличии ключевой 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. 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”. 2010. № 673. С. 365-374.

Поступила в редколлегию 13.09.2015

Баранник Владимир Викторович, д-р техн. наук, профессор, начальник кафедры автоматизированных систем управления, Харьковский университет Воздушных Сил им. И. Кожедуба. Научные интересы: кодирование и защита информации для передачи в телекоммуникационных системах. Адрес: Украина, 61000, Харьков, ул. Сумская, 77/79. E-mail: barannik_v_v@mail.ru.

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

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