УДК 629.391

В.В. БАРАННИК, А.Э. БЕКИРОВ

МЕТОД ФОРМИРОВАНИЯ ФУНКЦИОНАЛА СТЕГАНОГРАФИЧЕСКОГО КОДИРОВАНИЯ, УСТОЙЧИВОГО К СТЕГАНО-АТАКАМ

Анализируются недостатки непосредственного встраивания информации на различные позиции элементов пространственно-временного представления изображения-контейнера. Для устранения выявленных недостатков предлагается использовать функционал от числа с встроенной информацией. Приводятся требования к синтезированному функционалу.

1. Введение

Современное развитие инфокомунникационных сетей диктует новые требования к безопасности информационных ресурсов. Одним из возможных путей решения данной проблемы является использование стеганографического встраивания для скрытия данных.

Наиболее распространенные стеганографические методы – это алгоритмы непосредственного встраивания информации в пространственно-временные элементы представления изображений. В связи с этим наиболее актуальными научно-прикладными исследованиями есть поиски новых подходов для разработки альтернативных стеганографических алгоритмов непосредственного встраивания.

Возможным решением проблемы улучшения показателей визуальной устойчивости стеганограммы, а также стойкости к трансформации и атакам является разработка преобразования для элемента с встроенными данными. Наряду с решением задачи повышения информационной безопасности такое преобразование также должно обеспечить компактное представление стеганограммы. *Цель* данного исследования состоит в разработке функционала от числа со встроенными данными и формулировке требований к такому функциональному преобразованию.

2. Анализ недостатков стеганографических систем (СС) встраивания на различные позиции элементов пространственно-временного представления изображений

Современные стеганографические системы разделяются на алгоритмы непосредственного встраивания и алгоритмы косвенного встраивания.

В методах непосредственного встраивания бит информационной последовательности скрываемого сообщения заменяется на бит данных изображения-контейнера (ИК).

Встраивание бита информационной последовательности скрываемого сообщения в косвенных методах осуществляется путем создания зависимости между некоторыми параметрами изображения контейнера по определенному алгоритму. Благодаря тому, что данный алгоритм заранее известен на приемной стороне, стегодекодер выделяет логический 0 или 1 бит встроенной информационной последовательности.

Для решения задач скрытого встраивания данных методы непосредственного встраивания имеют ряд преимуществ. В сравнении с методами косвенного встраивания алгоритмы непосредственного встраивания характеризуются:

– простотой реализации алгоритма;

– большим объемом встраиваемых данных $W_{встр}$;

– небольшими значениями временных затрат на реализацию встраивания и извлечения, при которых время встраивания $\tau_{(W_{встр})пр}$ и время изъятия $\tau_{(W_{встр})обр}$ является наименьшим;

– отсутствием необходимости предварительной обработки изображения-контейнера и скрываемого сообщения.

Непосредственное встраивание СС может осуществляться как в пространственно-временную, так и в частную область ИК. Как правило, такое встраивание проводится в

отдельный элемент текущего представления ИК (рис. 1), точнее в отдельные биты элемента. В данном случае элемент представляет собой двоичное позиционное число A_2 с основанием, равным двум, т.е. $A_2 = [A]_2$.

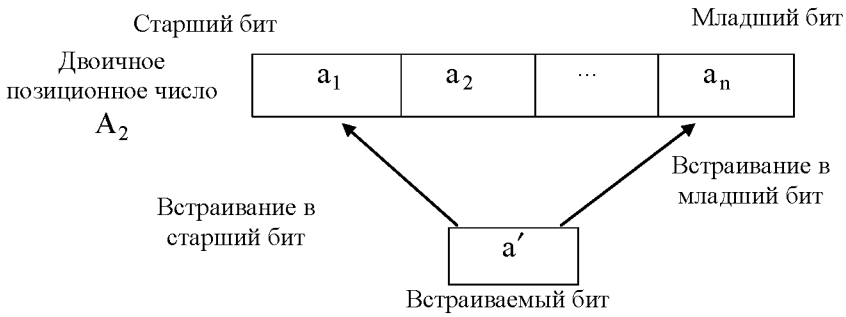

Рис. 1. Схема встраивания бита СС в элемент текущего представления ИК

Процесс непосредственного встраивание фактически представляет собой замену одного бита исходного элемента-контейнера на бит скрываемого сообщения с использованием некоторого функционала φ_2, условия или правила.

В существующих стегнаографических методах наиболее проработанные подходы основываются на встраивании информации в наименее значимый младший (НМЗ) бит. В связи с этим рассмотрим характеристики таких стеганосистем.

Метод встраивания в наименее значащий бит осуществляет замену младшего бита a_n двоичного позиционного числа A_2 на бит b_ξ встраиваемого сообщения B (рис. 2). Это описывается следующим выражением:

$$a'_n = b_\xi,\ A'_2 = \{a_1, a_2, a_{n-1}, a'_n\},$$

где A'_2 – число, содержащее встроенный бит a'_n скрываемого сообщения.

Здесь b_ξ – ξ-й элемент встраиваемой двоичной последовательности $B = \{b_1;...;b_\xi;...;b_\nu\}$, $a'_i \in [0;1]$; $b_\xi \in [0;1]$, $i = \overline{1,\nu}$; $\xi = \overline{1,\nu}$.

Такой подход для встраивания скрываемой информации характеризуется тем, что количественная метрика $\varepsilon(A;A')$, указывающая на степень отличия между значением элемента A исходного изображением до встраивания информации (изображение-контейнер) и значением A' этого же элемента изображения со встроенной информацией (стеганограммой), будет наименьшей: $\varepsilon(A;A') \to 0$.

В то же время данный принцип встраивания отличается низкой устойчивостью стеганограммы относительно трансформирующих и атакующих воздействий. В этом случае вероятность $P_{из}$ того, что элемент b_ξ скрываемого сообщения будет изъят без ошибок, стремится к нулю, т.е. $P_{из}(b'_\xi = b_\xi) \to 0$, или соответственно вероятность $\overline{P}_{из}$ того, что элемент b_ξ скрываемого сообщения изъят с ошибкой, будет наибольшей $P_{из}(b'_\xi \neq b_\xi) \to 1$.

Здесь b'_ξ – значение ξ-го элемента скрываемого сообщения, который изымается при наличии трансформирующего или атакующего воздействия; $(b'_\xi = b_\xi)$ – событие, состоящее в том, что значения b_ξ элемента скрываемого сообщения до атаки и полученного b'_ξ после атаки будут равными; $(b'_\xi \neq b_\xi)$ – событие, состоящее в том, что значение элемента скрываемого сообщения до атаки b_ξ и полученного после атаки b'_ξ будут неравными.

Другими словами, если использовать количественную метрику $\delta(B'_2;B_2)$, указывающую на степень отличия между исходным сообщением B и изъятым на приемной стороне сообщением B'_2, то будет выполняться соотношение $\delta(B'_2;B_2) \to \max$.

Наоборот, метод встраивания элемента скрываемого сообщения в старший бит исходного числа A_2, т.е. $A'_2 = \{a'_1, a_2, a_n\}$; $a'_1 := b_\xi$, повышает стойкость встроенных данных к трансформации и атакам. Тогда вероятность $P_{из}$ того, что элемент b_ξ скрываемого сообщения изъят без ошибок, будет наибольшей, т.е. $P_{из}(b'_\xi = b_\xi) \to 1$, а вероятность $\overline{P}_{из}$ того, что элемент b_ξ скрываемого сообщения изъят с ошибкой, будет наименьшей, т.е. $P_{из}(b'_\xi \neq b_\xi) \to 0$.

Здесь A'_2 – число-стеганограмма, содержащее встроенный бит a'_1 скрываемого сообщения; b_ξ – ξ-й элемент встраиваемой двоичной последовательности $B_2 = \{b_1; \ldots; b_\xi; \ldots; b_\nu\}$, $a'_i \in [0; 1]$; $b_\xi \in [0; 1]$; $i = \overline{1, \nu}$; $\xi = \overline{1, \nu}$; b'_ξ – элемент сообщения, изъятый при наличии атакующего воздействия.

Однако такое встраивание вносит существенные искажения с позиции визуального восприятия ИК. Здесь значение количественной метрики $\varepsilon(A; A')$ будет наибольшей, т.е. $\varepsilon(A; A') \to \max$.

Обобщенно недостатки непосредственного встраивания бита СС в элемент контейнер задаются следующим соотношением:

$$a'_\tau := \begin{cases} b_\xi \;\&\; P_{из}(b'_\xi = b_\xi) \to 0 \;\&\; \varepsilon(A; A') \to 0 \;\&\; \delta(B'_2; B_2) \to \max, \;\; \tau \to n; \\ b_\xi \;\&\; P_{из}(b'_\xi = b_\xi) \to 1 \;\&\; \varepsilon(A; A') \to \max \;\&\; \delta(B'_2; B_2) \to 0, \;\; \tau \to 1. \end{cases}$$

При встраивании бита СС в старший бит исходного числа наблюдается стойкость встроенных данных при значительных визуальных искажениях, и наоборот, встраивание СС в младший бит характеризуется низкой стойкостью встроенных данных при минимальных визуальных искажениях.

3. Разработка модели функционального преобразования для непосредственного встраивания данных

Для устранения выявленных недостатков, т.е. обеспечения визуальной устойчивости стеганограммы, при которой значение количественной метрики $\varepsilon(A; A')$ будет наименьшим, т.е. $\varepsilon(A; A') \to 0$, и устойчивости к трансформации и атакам предлагается синтезировать функционал $f(A')$ от *числа* со встроенной информацией. Такой функционал должен обеспечить следующие требования:

1) Компактное представление стеганограммы C, полученной после функционального преобразования $f(A')$, т.е. $C = f(A')$.

Здесь требуется обеспечить выполнение условия, когда объем $W(C)$ сжатого представления после функционального преобразования не будет превышать объем $W(A)$ сжатого представления той же последовательности A до функционального преобразования, т.е. будет выполняться условие: $W(C) \le W(A)$.

Другими словами, функциональное преобразование не должно влиять в первую очередь на изменение тех закономерностей, которые будут учитываться в процессе дальнейшей компрессии.

2) Взаимооднозначность прямого $f(A')$ и обратного $f^{(-1)}(C)$ преобразований. В этом случае должен существовать обратный функционал $f^{(-1)}(C)$, позволяющий авторизированному пользователю получить скрываемое сообщение без потери информации, т.е. количественная метрика $\delta(B'_2; B_2)$, указывающая на степень отличия между исходным сообщением B_2 и изъятым на приемной стороне сообщением B'_2, будет принимать нулевое значение $\delta(B'_2; B_2) = 0$.

3) Возможность осуществлять обратное преобразование (реконструкцию) по биполярному принципу. Биполярность заключается в том, что для функционала $f(A')$ существует два варианта обратного преобразования. Первый вариант является стандартным. Он

используется неавторизированным пользователем (злоумышленником), а восстановление изображения осуществляется для стандартных условий $\Psi^{(1)}$, необходимых для достоверной реконструкции элементов изображения-контейнера (позиционного числа):

$$A(1)'' = f^{(-1)}(C; \Psi^{(1)}).$$

Для такого варианта должно обеспечиваться отсутствие визуальных искажений в реконструируемом изображении, что задается условием, при котором значение количественной метрика $\varepsilon(A; A(1)'')$ будет наименьшим:

$$\varepsilon(A; A(1)'') \to 0, \text{ где } A(1)'' = f^{(-1)}(C; \Psi^{(1)}),$$

и блокирование возможности успешного стеганоанализа и изъятия сообщения. Условия блокирования изъятия встроенного сообщения задается следующим соотношением:

$$\delta(B_2''; B_2) \to \max,$$

здесь B_2'' – скрываемое сообщение, полученное при декодировании неавторизированным пользователем.

Второй вариант, наоборот, существует для авторизированного пользователя. Здесь обратное функциональное преобразование осуществляется с использованием ключа $\Psi^{(2)}$ или по определенному условию, известному авторизированным пользователям, так что $\Psi^{(2)} \neq \Psi^{(1)}$, т.е. $A(2)'' = f^{(-1)}(C; \Psi^{(2)})$.

В процессе этого формируется число-стеганограмма $A(2)''$, так чтобы:

– обеспечивалось безошибочное изъятие по известному оператору $\varphi^{(-1)}$ (оператору выборки элемента) встраиваемого элемента b'_ξ скрываемого сообщения, т.е. $b'_\xi = \varphi^{(-1)}(A(2)'')$ и $\delta(B'_2; B_2) = 0$;

– метрика $\varepsilon(A; A(2)'')$, указывающая на степень отличия между числом A, составленным для исходного изображения до встраивания информации (изображение-контейнер) и числом $A(2)''$ соответствующего изображения со встроенной информацией (стеганограммой), принимала наименьшее значение, т.е. $\varepsilon(A; A(2)'') \to 0$.

Процесс изъятия элемента b'_ξ скрываемого сообщения B' описывается соотношением

$$b'_\xi = \varphi^{(-1)}(f^{(-1)}(C)).$$

Здесь $\varphi^{(-1)}$ – оператор изъятия.

Формула, которая описывает реконструкцию числа $A(2)''$ на приемной стороне по известной стеганограмме и ключевой информации, имеет вид:

$$A(2)'' = f^{(-1)}(C; \Psi^{(2)}).$$

При изъятии встроенной информации авторизированным пользователем количественная метрика $\delta(B'_2; B_2)$, указывающая на степень отличия между исходным встраиваемым сообщением B и изъятым на приемной стороне сообщением B', будет принимать нулевое значение: $\delta(B'_2; B_2) = 0$.

Требование биполярности можно обобщить следующей системой выражений:

$$A(\gamma)'' = f^{(-1)}(C; \Psi^{(\gamma)}),$$

$$\delta(B'; B) \to \begin{cases} \max, & \to \gamma=1 \ \& \ \Psi = \Psi^{(1)}; \\ 0, & \to \gamma=2 \ \& \ \Psi = \Psi^{(2)}. \end{cases}$$

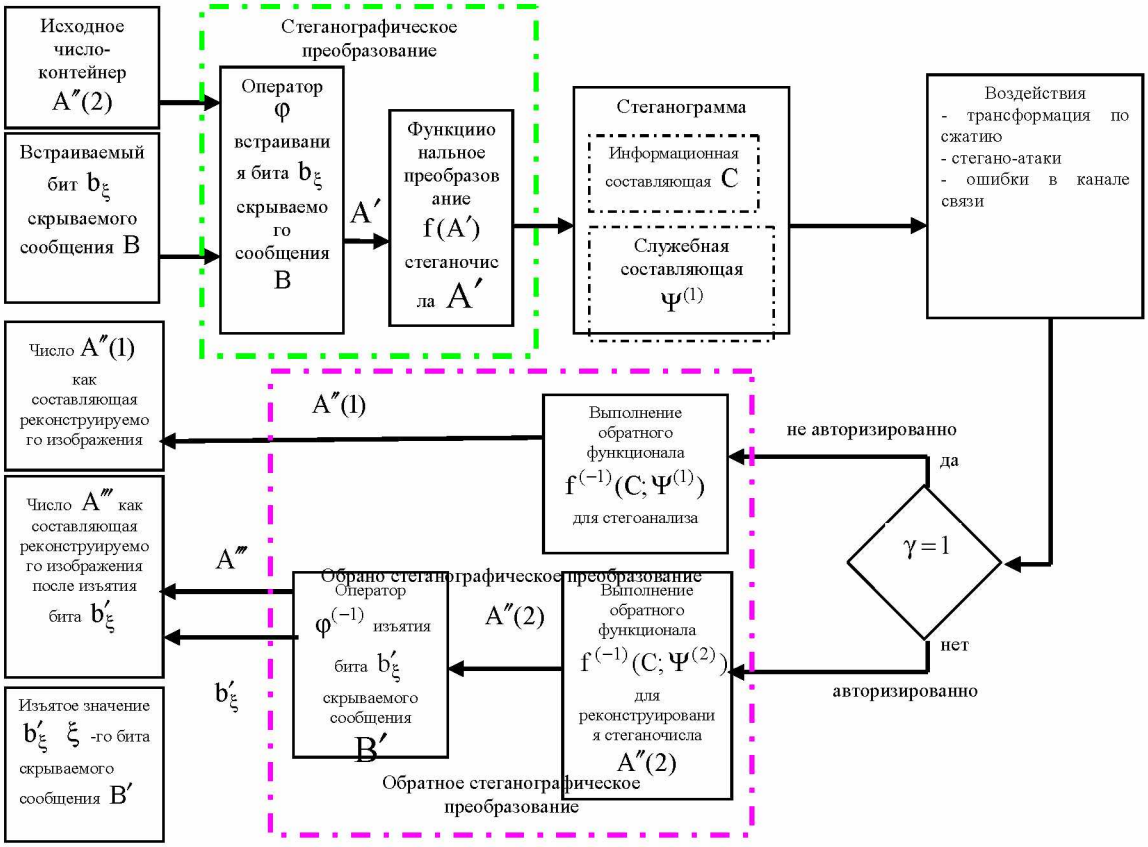

Рис. 2. Схема стеганографического преобразования на основе использования функционала для стегочисла

4) Функциональное преобразование должно быть инвариантным к атакующим воздействиям (ошибки в канале связи, пережатие ДКП с квантованием). Должна обеспечиваться устойчивость скрываемого сообщения, т.е. возможность его достоверного (целостного) изъятия в случае последующего сжатия, проведения атак и воздействия ошибок канала связи. Другими словами, количественная метрика $\alpha(A; A'')$, указывающая на степень отличия между числом A, составленным для исходного изображениия при отсутствии атакующего воздействия (изображение-контейнер), и числом A'', соответствующим изображению со встроенной информацией при наличии атакующего воздействия, должна быть наименьшей

4. Выводы

Разработан подход для улучшения характеристик непосредственного стеганографического встраивания, включающий в себя синтезирование функционала от элемента со встроенным битом скрываемого сообщения. Сформулированы требования для такого функционального преобразования. Синтезированный функционал должен обеспечить:

1) компактное представление стеганограммы, полученное после функционального преобразования;

2) взаимооднозначность прямого и обратного преобразований. В этом случае должен существовать обратный функционал, позволяющий авторизированному пользователю получить скрываемое сообщение без потери информации;

3) возможность осуществлять обратное преобразование по биполярному принципу. Биполярность функционала заключается в существовании двух вариантов обратного преобразования для авторизированного пользователя и для злоумышленника;

4) инвариантность к атакующим воздействиям, т.е. обеспечивать устойчивость скрываемого сообщения в условиях сжатия, проведения атак и помех в каналах связи.

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