УДК 681.3

В. В. БАРАННИК[1], Ю. Н. РЯБУХА[1], А. Э. БЕКИРОВ[2]

[1] *Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков*
[2] *Харьковский национальный университет радиоэлектроники, Харьков*

ТЕХНОЛОГИЯ НЕРАВНОВЕСНОГО ПОЗИЦИОННОГО КОДИРОВАНИЯ ДЛЯ ФУНКЦИОНАЛЬНОГО ПРЕОБРАЗОВАНИЯ ЧИСЕЛ СО ВСТРОЕННОЙ ИНФОРМАЦИИ

В данной статье предложен подход для повышения информационной безопасности на основе использования методов цифровой стеганографии. Проводится анализ недостатков существующих методов непосредственного встраивания информации в изображение-контейнер. Для повышения визуальной устойчивости существующих методов встраивания вводится функционал от числа со встроенной информацией. Также формулируются требования для функционального преобразования числа со встроенной информацией. Для соответствия требованиям визуальной устойчивости стеганочисла, устойчивости к трансформированию и атакам сформулирован подход для функционального преобразования на основе неравновесного позиционного кодирования.

Ключевые слова: *цифровая стеганография, алгоритмы встраивания, визуальная устойчивость, стеганограмма, неравновесное позиционное число, неравновесное позиционное кодирование.*

Введение

Одним из возможных способов скрытой передачи данных в инфокомунникационных каналах связи является передача данных, стеганографически встроенных в контейнер. Стеганографические алгоритмы позволяют избежать прямых атак на закрытую информацию, поскольку злоумышленнику не известно, присутствует ли такая информация в потоке данных и что является ее цифровым носителем. Наиболее распространенными алгоритмами встраивания являются методы встраивания в изображение-контейнер [1 – 4].

Существующие стеганографические методы не в полной мере удовлетворяют требованиям информационной безопасности. Успешность применения конкретного алгоритма встраивания для скрытой передачи данных зависит от конкретных условий его функционирования. Для современных стеганографических методов на основе изображения существует необходимость повышения визуальной устойчивости изображения со встроенными данными (стеганограммы). Такое повышение достигается путем уменьшения количества модифицированных элементов исходного изображения-контейнера. Однако такой подход негативно отражается на объеме встраиваемых данных. Наоборот, улучшение характеристик стеганографических методов с позиции объема встраиваемых данных неизбежно влечет за собой увеличение модифицированных элементов стеганограммы, что также негативно отражается на ее визуальной устойчивости. Отсюда возникает необходимость повышения устойчивости стеганограммы при заданном объеме встраиваемых данных.

Анализ существующих методов непосредственного встраивания

Наиболее распространенными стеганографическими методами встраивания информации в изображение контейнер являются алгоритмы непосредственного встраивания в элементы пространственного представления контейнера (рис. 1) [3 - 5]. В данном случае элемент представляет собой двоичное позиционное число A_2 с основанием равным двум, т.е. $A_2 = [A]_2$, а процесс непосредственного встраивания фактически представляет собой замену одного бита исходного элемента-контейнера на бит скрываемого сообщения с использованием некоторого функционала, условия или правила.

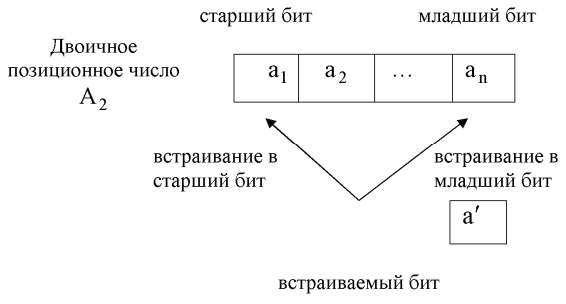

Рис. 1. Схема встраивания бита секретного сообщения в элемент текущего представления изображения контейнера

Такое встраивание возможно на различные позиции исходных элементов контейнера.

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

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

где A'_2 - число, содержащее встроенный бит a'_n скрываемого сообщения;

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 изображения до встраивания информации (изображение-контейнер) и значением A' этого же элемента изображения со встроенной информацией (стеганограммой) будет наименьшей:

$$\varepsilon(A; A') \to 0.$$

В тоже 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

$$P_{из}(b'_\xi \neq b_\xi) \to 1,$$

где 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.

Наоборот метод встраивания элемента скрываемого сообщения в старший бит исходного числа A_2, т.е.

$$A'_2 = \{a'_1, a_2, a_n\}; \quad a'_1 := b_\xi$$

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.

$$P_{из}(b'_\xi = b_\xi) \to 1,$$

где A'_2 - число-стеганограмма, содержащее встроенный бит a'_1 скрываемого сообщения;

b_ξ - ξ-й элемент встраиваемой двоичной последовательности $B_2 = \{b_1; ...; b_\xi; ...; b_\nu\}$, $a'_i \in [0; 1]$; $b_\xi \in [0; 1]$; $i = \overline{1, \nu}$; $\xi = \overline{1, \nu}$;

b'_ξ - элемент сообщения, изъятый при наличии атакующего воздействия.

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

$$\varepsilon(A; A') \to \max.$$

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

Основная часть

Для устранения выявленных недостатков, т.е. обеспечения визуальной устойчивости стеганограммы необходимо 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:

$$W(C) \le W(A).$$

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 метрики $\varepsilon(A; A(1)'')$ 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, полученный 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 $\Psi^{(2)} \ne \Psi^{(1)}$, т.е.

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

В процессе чего формируется число-стеганограмма $A(2)''$, так чтобы выполнялись следующие условия:

- обеспечивалось безошибочное изъятие по известному оператору $\varphi^{(-1)}$ (оператору выборки элемента) встраиваемого элемента b_ξ' скрываемого сообщения, т.е.

$$b_\xi' = \varphi^{(-1)}(A(2)'') \quad \text{и} \quad \delta(B_2'; B_2) = 0;$$

- метрика $\varepsilon(A; A(2)'')$, указывающая на степень отличия между числом A, составленным для исходного изображения до встраивания информации (изображение-контейнером) и числом $A(2)''$ соответствующего изображению 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

$$b_\xi' = \varphi^{(-1)}(f^{(-1)}(C)),$$

где $\varphi^{(-1)}$ - 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 ме-

жду исходным встраиваемым сообщением B и изъятым на приемной стороне сообщением B', будет принимать нулевое значение:

$$\delta(B_2'; B_2) = 0.$$

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.

Таким образом, необходимо разработать подход для функционального преобразования числа со встроенной информацией на основе функционала, обладающего свойствами, соответствующими требованиям визуальной устойчивости стегонограммы.

Для соответствия требованиям визуальной устойчивости стеганочисла A', устойчивости к трансформированию и атакам, синтезированный функционал $f(A')$ должен обладать следующими свойствами:

1) формирование стеганограммы C с использованием стеганообразующего функционала должно осуществляться по интегральному принципу в два этапа. На первом этапе как результат применения функционала $f(A')$ к стеганочислу A' формируется кодовое значение N, содержащее информацию об элементах числа A', т.е.

$$N = f(A').$$

На основе сформированного значения N на втором этапе строится результирующее кодовое представление C стеганограммы

$$C_2 = \varphi_c(N),$$

где φ_c - оператор, обеспечивающий построение двоичного кода C_2 для кодового значения N.

В этом случае получим

$$C_2 = \{c_1; ...; c_q; ...; c_Q\}, \quad c_q \in \{0; 1\},$$

где Q - количество бит на представления стеганограммы C_2;

2) количественная метрика $\varepsilon(A(1)''; A(2)'')$ указывающая на степень отличия числа $A(1)''$, восстановленного при стандартных условиях $\Psi^{(1)}$ неавторизированным пользователем

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

и числа $A(2)''$, реконструированного авторизированным пользователем с использованием ключа $\Psi^{(2)}$

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

не должна превышать значения порога визуальной незначимости μ, т.е.

$$\varepsilon \in 0...\mu;$$

3) стеганограмма C, должна содержать сведения о векторе служебной информации $\Psi^{(1)}$, при наличии которой возможна реконструкция элементов $A(1)''$ изображения контейнера при отсутствии информации о наличии встроенного сообщения

$$C_2 = \varphi_c(N, \Psi^{(1)}) \qquad A(1)'' = f^{(-1)}(C; \Psi^{(1)});$$

4) извлечения элемента b_ξ' скрываемого сообщения B_2' противником, при наличии у него информации о наличии встраивания, возможно только при известном ключе $\Psi^{(2)}$ (ключевой информации). Такая ключевая информация может представлять собой условия, с учетом которых происходило встраивание скрываемого сообщения или же принимать значение некоторого симметричного ключа $\Psi^{(2)}$ известного на приемной и передающее стороне. Выражение, описывающее выполнение обратного функционала будет иметь вид

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

5) служебная составляющая $\Psi^{(1)}$ должна иметь определяющее значение при формировании кодограммы таким образом, чтобы безошибочная реконструкция исходного изображения $A(1)''$ для неавторизированного пользователя достигалась только при наличии полных сведений о векторе служебных данных, т.е. если $\Psi^{(1)'} \neq \Psi^{(1)}$, то

$$C_2' = \varphi_c(N, \Psi^{(1)'}) \text{ и } A(1)'' \neq f^{(-1)}(C; \Psi^{(1)'}),$$

где $C_2 \neq C_2'$; C_2' - значение двоичного кодового слова, восстановленного в результате использования

вектора $\Psi^{(1)'}$ служебных данных, декодированных с ошибкой;

6) в результате применения функционала $f(A')$ должно формироваться компактное представление стеганограммы C. Другими словами, в процессе стеганографического преобразования ликвидируется избыточность.

В качестве преобразующего функционала, обладающего свойствами для соответствия требованиям относительно процесса скрытия данных предлагается использовать кодообразующую функцию для неравновесного позиционного числа (НПЧ кодирование), а в качестве элемента-контейнера предлагается использовать неравновесное позиционное (НП) число.

В процессе неравновесного позиционного кодирования формируются кодовые комбинации, состоящие из двух частей, а именно: информационная составляющая N и служебная составляющие Ψ (рис 2).

Рис.2 . Схема кодограммы для неравновесного позиционного числа

В этом случае исходный элемент изображения рассматривается как неравновесное позиционное числа A, состоящее из r элементов, а именно

$$A = \{a_1;...; a_{i,j};...;a_{i,r}\}.$$

Для исходного НП числа A значения кода определяется по формуле:

$$N = f'(A),$$

где N- код исходного неравновесного позиционного числа A.

На втором этапе для сформированного значения кода N строится результирующее кодовое представление C_2 неравновесного позиционного числа A (рис. 3):

$$C_2 = \varphi_c(N, \Psi),$$

где φ_c - оператор, обеспечивающий построение двоичного кода C_2 для кодового значения N и служебных данных Ψ .

В этом случае получим

$$C_2 = \{c_1;...;c_q;...;c_Q\}, \quad c_q \in \{0; 1\},$$

где Q - количество бит на представления НП числа C_2.

Служебная составляющая включает в себя информацию о системе оснований неравновесного позиционного числа $\Psi = \{\psi_{i,j}\}$.

В случае такого подхода для формирования кодового представления C_2 неравновесного позиционного числа A, оператор обратного функционального преобразования $f^{(-1)'}(\bullet)$ позволит получить исходное НП число A при наличии служебной информации Ψ. Выражение, которое описывает обратное функциональное преобразование, имеет вид:

$$A = f^{(-1)'}(C_2; \Psi).$$

Для такого подхода принцип встраивания предлагается выбирать следующим образом (рис. 4).

В исходное неравновесное позиционное числа A при помощи оператора φ' встраивается бит b_ξ скрываемого сообщения B таким образом, что

$$A' = \varphi'(A; b_\xi),$$

где A' - неравновесное позиционное число с встроенным битом b_ξ (НП стеганочисло).

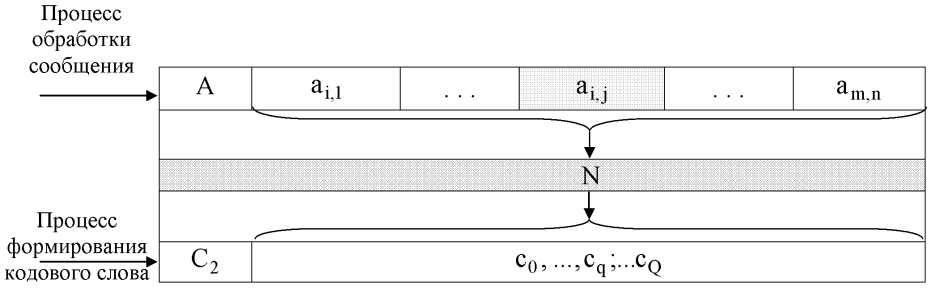

Рис. 3. Структурная схема построения кодовых конструкций для неравновесного позиционного числа A

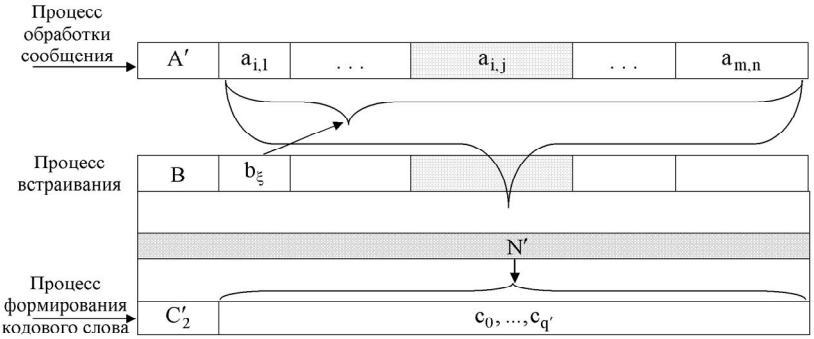

Рис. 4. Структурная схема построения кодовых конструкций НП стеганочисла A'

Затем определяется код N' для числа A':

$$N' = f'(A').$$

На третьем этапе для сформированного значения кода N' строится результирующее кодовое представление C'_2 неравновесного позиционного стеганочисла A'

$$C'_2 = \varphi_c(N', \Psi^{(1)}),$$

где φ_c - оператор, обеспечивающий построение двоичного кода C'_2.

Обратное стеганографическое преобразование будет выполняться по биполярному принципу для авторизированного (при наличии ключа $\Psi^{(2)}$) и неавторизированного пользователя (злоумышленника) при стандартных условиях.

Первый способ используется неавторизированным пользователем. Восстановление изображения происходит при наличии открытой служебной информации $\Psi^{(1)}$, представляющей собой систему оснований НП числа A'. Такое обратное преобразование позволяет достоверно реконструировать элемент $A''(1)$ по формуле:

$$A(1)'' = f'^{(-1)}(C_2; \Psi^{(1)})$$

так, чтобы значение количественной метрики $\varepsilon(A; A(1)'')$ было наименьшей

$$\varepsilon(A; A(1)'') \to 0,$$

где $A''(1)$ - элемент, реконструированный при стандартных условиях.

Второй способ существует для авторизированного пользователя. Здесь обратное функциональное преобразование осуществляется с использованием открытой служебной информации $\Psi^{(1)}$ и ключа $\Psi^{(2)}$. В данном случае значение ключа $\Psi^{(2)}$ представляет собой заранее известное значение основания встроенного элемента так, чтобы $\Psi^{(2)} \neq \Psi^{(1)}$. Обратное функциональное преобразование позволит авторизированному пользователю безошибочно реконструировать стеганочисло, т.е.

$$A(2)'' = f'^{(-1)}(C_2; \Psi^{(1)}; \Psi^{(2)}) \quad \text{и} \quad A(2)'' = A',$$

где $A(2)''$ - НП число с встроенными данными, полученное при обратном функциональном преобразовании авторизированным пользователем.

Изъятие встроенной информации происходит без внесения ошибок вследствие применения оператора изъятия φ_c^{-1} к реконструируемому НП стеганочислу $A(2)''$ при котором также возможно безошибочное восстановление числа A''' как элемента исходного изображения, так что:

$$\varphi'^{(-1)}(A''(2)) = \begin{cases} b'_\xi, \; b'_\xi = b_\xi; \\ A''', \quad A''' = A. \end{cases}$$

На рисунке 5 отображена схема стеганографического метода на основе неравновесного позиционного кодирования. Прямое стеганографическое преобразование реализуется в три этапа. На первом этапе при помощи оператора встраивания φ бит b_ξ скрываемого сообщения B_2 встраивается на различную позицию НП числа A. Полученное вследствие загрузки бита b_ξ неравновесное позиционное A' определяется выражением

$$A' = \varphi(b_\xi; A).$$

На втором этапе для стеганочисла A' по правилу $f(A')$ формируется код N':

$$N' = f'(A').$$

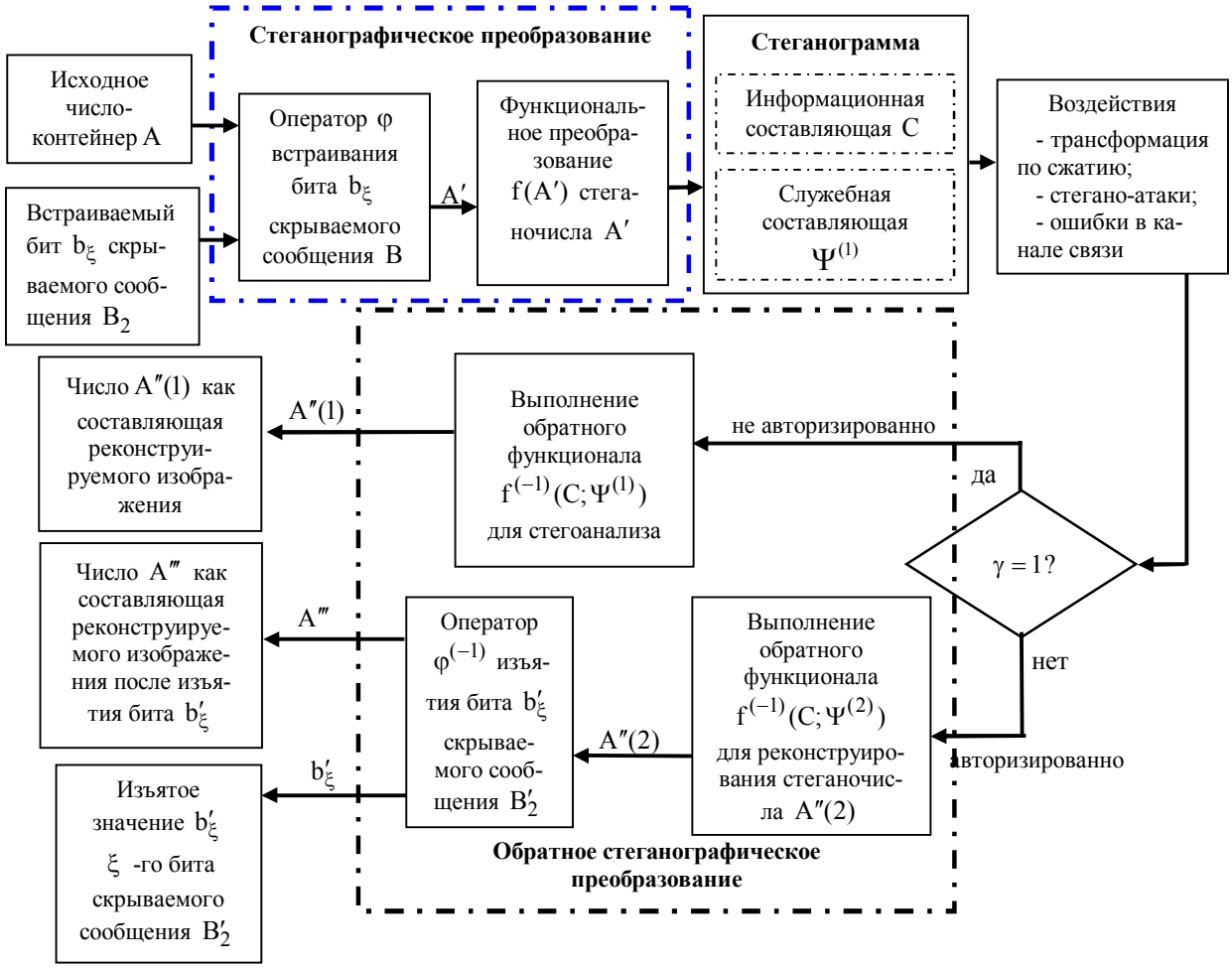

Рис. 5. Схема стеганографического преобразования на неравновесное позиционное кодирование

Формирование кода происходит с учетом ключевой информации $\Psi^{(2)}$, подразумевающей под собой основание встроенного элемента.

На третьем этапе строится результирующее кодовое представление C'_2 стеганочисла A'. Это описывается выражением

$$C'_2 = \varphi_c(N';\Psi^{(1)}).$$

Полученная стеганограмма C, содержащая в себе информационную составляющую N' и служебную составляющую $\Psi^{(1)}$, подвергается атакующим воздействиям.

Обратное стеганографическое преобразование включает в себя случай для неавторизированного пользователя (стегоанализ) при условии, что ему известен обратный функционал $f'^{(-1)}$, и авторизированного пользователя. При стегоанализе, по правилу $f'^{(-1)}(\bullet)$ формируется число

$$A''(1) = f'^{(-1)}(C'_2;\Psi^{(1)}).$$

Здесь $A''(1)$ - число, как составляющая реконструируемого изображения, полученное в результате стегоанализа.

Для авторизованного пользователя обратное стеганографическое преобразование происходит в два этапа. На первом этапе по правилу $f'^{(-1)}(\bullet)$ и с учетом ключевой информации $\Psi^{(2)}$ происходит реконструкция стеганочисла

$$A''(2) = f'^{(-1)}(C'_2;\Psi^{(1)};\Psi^{(2)}).$$

На втором этапе из реконструированного стеганочисла $A''(2)$ происходит изъятие b'_ξ скрываемого сообщения B_2. В результате применения оператора изъятия $\varphi^{(-1)}$ также происходит реконструкция числа A''', как составляющего исходного изображения, что описывается выражением

$$\varphi^{(-1)}(A'(2)) = \begin{cases} b'_\xi; \\ A'''. \end{cases}$$

Выводы

Предложен подход для повышения информационной безопасности систем специального назначения с использованием систем стеганографического встраивания информации в изображение контейнер.

Проведен анализ недостатков непосредственного встраивания на различные позиции пространственно-временного представления изображения-контейнера. Для устранения выявленных недостатков обоснована необходимость применения функционального преобразования от числа со встроенной информацией. Сформулированы требования к синтезированному функционалу.

Определена система свойств, которой должен обладать синтезированный функционал, для соответствия требованиям визуальной устойчивости к трансформированию и атакам.

Обоснован подход для функционального преобразования числа со встроенной информацией на основе неравновесного позиционного кодирования.

Литература

1. Грибунин, В. Г. Цифровая стеганография [Текст] / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – М. :Солон-Пресс, 2009. – 265 с.

2. Рябко, Б. Я. Основы современной криптографии и стеганографии [Текст] / Б. Я. Рябко, А. Н. Фионов. – М. : Горячая линия–Телеком, 2010. –232 с.

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

4. Fridrich, J. Steganographyin Digital Media Principles, Algorithms, and Applications [Text] / J. Fridrich. – Cambridge UnivP, 2010. – 462 p.

5. Luo, W. Edge Adaptive Image Steganography Based on LSB Matching Revisited [Text] / W. Luo, F. Huang, J. Huang // Transactions on Information Forensics and Security. – 2010. – Vol. 5. – P. 201-214.

Надійшла до редколегії 15.04.2014, рассмотрена на редколлегии 18.11.2014

Рецензент: д-р техн. наук, проф., заведующий кафедрой сети связи В. М. Безрук, Харьковский национальный университет радиоэлектроники, Харьков.

ТЕХНОЛОГІЯ НЕРІВНОВАГОВОГО ПОЗИЦІЙНОГО КОДУВАННЯ ДЛЯ ФУНКЦІОНАЛЬНОГО ПЕРЕТВОРЕННЯ ЧИСЕЛ З ВБУДОВУВАНОЮ ІНФОРМАЦІЄЮ

В. В. Бараннік, Ю. М. Рябуха, А. Е. Бекиров

Запропоновано підхід для підвищення інформаційної безпеки на основі використання методів цифрової стеганографії. Проводиться аналіз недоліків існуючих методів безпосереднього вбудовування інформації в зображення-контейнер. Для підвищення візуальної стійкості існуючих методів вбудовування вводиться функціонал від числа з вбудовуваною інформацією. Для відповідності вимогам візуальної стійкості стего-числа, стійкості к трансформуванню та атакам обґрунтовано підхід для функціонального перетворення на основі нерівновагового позиційного кодування.

Ключові слова: цифрова стеганографія, візуальна стійкість, алгоритми вбудовування, стеганограма, нерівновагове позиційне число, нерівновагове позиційне кодування.

TECHNOLOGY OF NONEQUILIBRIUM POSITIONAL CODING FOR THE FUNCTIONAL NUMBER CONVERSION WITH EMBEDDED DATA

V. V. Barannik, Yu. M. Ryabukha , A. E. Bekirov

Approach for increase of information security on the basis of digital steganography methods using is offered. The shortcomings analysis of existing direct embedding information methods in the image container is carried out. For visual stability increasing of existing methods of embedding the functionality from number with embedded information is entered. Requirements for the functional conversion of number with embedded information are formulated. For compliance to requirements of visual stability steganonumber, resistance to transformation and attacks approach for the functional conversion on the basis of nonequilibrium positional coding is reasonable.

Key words: digital steganography, visual stability, steganogram, algorithms of embedding, nonequilibrium positional number, nonequilibrium positional coding.

Баранник Владимир Викторович – д-р техн. наук, професор, начальник кафедры автоматизированных систем управления, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

Рябуха Юрий Николаевич – канд. техн. наук, соискатель, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

Бекиров Али Энверович – соискатель, Харьковский национальный университет радиоэлектроники, Харьков.