УДК 681.3

А.Е. Бекіров

Харківський національний університет радіоелектроніки, Харків

МЕТОД ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ СТЕГАНОГРАФІЧНИХ СИСТЕМ

В даній статті запропоновано підхід для підвищення інформаційної безпеки на основі використання методів цифрової стеганографії. Проводиться аналіз недоліків існуючих методів безпосереднього вбудовування інформації на різні позиції просторово-часового представлення контейнера-зображення. Для підвищення візуальної стійкості існуючих методів вбудовування вводиться функціонал від числа з будованою інформацією. Вводиться система властивостей, якими повинен володіти функціонал від числа із вбудованою інформацією. Для відповідності вимогам візуальної стійкості стеганочисла, стійкості до трансформування і атак сформульовано підхід для функціонального перетворення на основі позиційного кодування.

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

Вступ

Одним з можливих способів скритної передачі даних в інфокомунікаційних каналах зв'язку являється передача даних стеганографічно вбудованих в контейнер. Стеганографічні алгоритми дають змогу уникнути прямих атак на закриту інформацію, так як зловмиснику невідомо, присутня така інформація в потоці даних та що являється ії цифровим носієм. Найбільш розповсюдженими алгоритмами вбудовування являються методи вбудовування в контейнер-зображення.

Існуючі стеганографічні методи не повною мірою задовольняють вимогам інформаційної безпеки. Для сучасних стеганографічних методів на основі зображення існує необхідність підвищення візуальної стійкості зображення з вбудованими даними (стеганограмми). Таке підвищення досягається шляхом зменшення кількості модифікованих елементів вихідного зображення-контейнера. Однак такий підхід негативно відбивається на обсязі вбудованих даних. Навпаки, поліпшення характеристик стеганографічних методів з позиції обсягу вбудованих даних неминуче тягне за собою збільшення модифікованих елементів стеганограмми, що також негативно відбивається на її візуальної стійкості. Звідси виникає необхідність підвищення стійкості стеганограмми при заданому обсязі вбудованих даних.

Аналіз існуючих методів безпосереднього вбудовування. Найбільш поширеними стеганографічними методами вбудовування інформації в зображення контейнер є алгоритми безпосереднього вбудовування в елементи просторового уявлення контейнера (рис.1). Процес безпосереднього вбудовування фактично являє собою заміну одного біта вихідного елемента-контейнера на біт приховуваного повідомлення з використанням деякого функціоналу, умови або правила. Таке вбудовування можливо на різні позиції вихідних елементів контейнера.

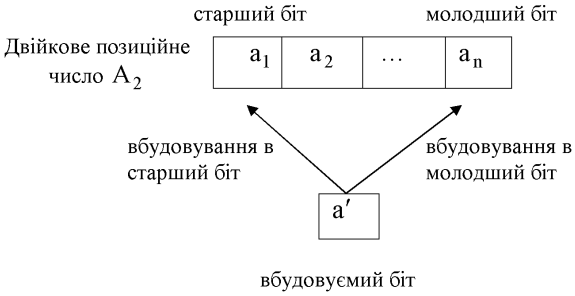

Рис. 1. Схема вбудовування біта секретного повідомлення в елемент поточного подання зображення контейнера

Метод вбудовування в найменш значущий біт здійснює заміну молодшого біта a_n двійкового позиційного числа A_2 на біт b_ξ вбудованого повідомлення B. Такий підхід для вбудовування прихованої інформації характеризується тим, що кількісна метрика $\varepsilon(A;A')$, яка вказує на ступінь відмінності між значенням елемента A вихідного зображенням до вбудовування інформації (зображення-контейнер) і значенням цього ж елемента зображення з вбудованою інформацією (стеганограммою) буде найменшою, $\varepsilon(A;A') \to 0$. У теж час даний принцип вбудовування відрізняється низькою стійкістю стеганограмми щодо трансформуючих і атакуючих дій. У цьому випадку ймовірність $P_{из}$ того, що елемент b_ξ приховуваного повідомлення буде вилучено без помилок прагне до нуля, тобто $P_{из}(b'_\xi = b_\xi) \to 0$, де b'_ξ - значення ξ-го елемента приховуваного повідомлення, який вилучається при наявності трансформуючого або атакуючого впливу; $(b'_\xi = b_\xi)$ - подія, яке складається у тому, що значення елемента b_ξ приховуваного повідомлення до атаки і отриманого b'_ξ після атаки будуть рівними;

Навпаки метод вбудовування елемента приховуваного повідомлення в старший біт вихідного числа підвищує стійкість вбудованих даних до трансформації і атак. Тоді ймовірність $P_{из}$ того, що елемент b_ξ приховуваного повідомлення вилучений без помилок, буде найбільшою, тобто $P_{из}(b'_\xi = b_\xi) \to 1$, Однак таке вбудовування вносить суттєві викривлення з позиції візуального сприйняття зображення-контейнера. Тут $\varepsilon(A; A')$ значення кількісної метрики буде найбільшою, тобто $\varepsilon(A; A') \to \max$. При вбудовуванні біта секретного повідомлення в старший біт вихідного числа спостерігається стійкість вбудованих даних при значних візуальних спотвореннях і навпаки, вбудовування секретного повідомлення в молодший біт характеризується низькою стійкістю вбудованих даних при мінімальних візуальних спотвореннях.

Основна частина

Для усунення виявлених недоліків, тобто забезпечення візуальної стійкості стеганограмми необхідно синтезувати функціонал f(A′) від числа з вбудованою інформацією. Такий функціонал повинен забезпечити такі вимоги:

1. Компактне представлення стеганограмми C, отриманої після функціонального перетворення f(A′). Тут потрібно забезпечити виконання умови, коли обсяг стисненого уявлення після функціонального перетворення W(C) не буде перевищувати обсяг стисненого уявлення W(A) тій же послідовності A до функціонального перетворення, тобто буде виконуватися умова: $W(C) \le W(A)$.

2. Бієктивне прямого f(A′) і зворотного $f^{(-1)}(C)$ перетворень. В цьому випадку повинен існувати зворотний функціонал $f^{(-1)}(C)$, що дозволяє авторизованому користувачеві отримати приховуване повідомлення без втрати інформації.

3. Можливість здійснювати зворотне перетворення (реконструкцію) по біполярному принципом. Біполярність полягає в тому, що для функціоналу f(A′) існує два варіанти зворотного перетворення. Перший варіант є стандартним. Він використовується неавторизованих користувачів (зловмисником), а відновлення зображення здійснюється для стандартних умов $\Psi^{(1)}$, необхідних для достовірної реконструкції елементів зображення-контейнера (позиційного числа) $A(1)'' = f^{(-1)}(C; \Psi^{(1)})$.

Другий варіант навпаки, існує для авторизованого користувача. Тут зворотне функціональне перетворення здійснюється з використанням ключа $\Psi^{(2)}$ або по певній умові відомої авторизованим користувачам, так що $\Psi^{(2)} \ne \Psi^{(1)}$, в процесі чого формується число-стеганограмма $A(2)''$, так щоб виконувалися наступні умови:

- забезпечувалося безпомилкове вилучення за відомим оператору $\varphi^{(-1)}$ (оператору вибірки елемента) вбудованого елемента b'_ξ приховуваного повідомлення;

- метрика $\varepsilon(A; A(2)'')$, що вказує на ступінь A відмінності між числом, складеним для вихідного зображенням до вбудовування інформації (зображення-контейнером) і числом $A(2)''$ відповідного зображенню з вбудованою інформацією (стеганограммой), брала найменше значення, тобто $\varepsilon(A; A(2)'') \to 0$.

Процес вилучення елемента b'_ξ приховуваного повідомлення B′ описується співвідношенням $b'_\xi = \varphi^{(-1)}(f^{(-1)}(C))$, де $\varphi^{(-1)}$ – оператор вилучення.

Формула, яка описує реконструкцію $A(2)''$ числа на приймальній стороні за відомою стеганограмме і ключової інформації має вигляд:

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

При вилученні вбудованої інформації авторизованим користувачем, кількісна метрика $\delta(B'_2; B_2)$, яка вказує на ступінь відмінності між вихідним вбудованим повідомленням B і вилученим на приймальній стороні B′ повідомленням, прийматиме нульове значення: $\delta(B'_2; B_2) = 0$.

4) Функціональне перетворення повинно бути інваріантним до атакуючих дій (помилки в каналі зв'язку, компресія ДКП з квантуванням).

В якості перетворюючого функціоналу, що володіє властивостями для відповідності вимогам щодо процесу приховування даних пропонується використовувати кодообразуючу функцію для нерівновагового позиційного числа (НПЧ кодування), а в якості елемента-контейнера пропонується використовувати нерівновагове позиційне (НП) число.

У процесі нерівновагового позиційного кодування формуються кодові комбінації, що складаються з двох частин, а саме: інформаційна складова N і службова складова Ψ.

У цьому випадку вихідний елемент зображення розглядається як нерівновагове позиційне число A, що складається з r елементів, а саме

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

Для вихідного НП числа значення коду визначається за формулою $N = f'(A)$. де N- код вихідного нерівновагового позиційного числа A. На другому етапі для сформованого значення коду N будується результуюче кодове подання C_2 нерівновагового позиційного числа A: $C_2 = \varphi_c(N, \Psi)$, де φ_c - оператор, що забезпечує побудову двійкового коду C_2 для кодового значення N і службових даних Ψ. У цьому випадку отримаємо

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

де Q - кількість біт на подання НП числа C_2.

Службова складова включає в себе інформацію про систему основ нерівновагового позиційного числа $\Psi = \{\psi_{i,j}\}$. У разі такого підходу для формування кодового представлення C_2 нерівновагового позиційного числа A, оператор зворотного функціонального $f^{(-1)'}(\bullet)$ перетворення дозволить отримати вихідне НП число A при наявності службової інформації. $\Psi^{(1)}$. Вираз, який описує зворотне функціональне перетворення, має вигляд:

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

Для такого підходу принцип вбудовування пропонується вибирати таким чином. У вихідне нерівновагове позиційне число A за допомогою оператора φ' вбудовується біт приховуваного b_ξ повідомлення таким чином, що $A' = \varphi'(A; b_\xi)$, де A' – нероівновагове позиційне число з вбудованим бітом b_ξ (НП стеганочисло). $N' = f'(A')$.

На третьому етапі N' для сформованого значення коду C'_2 будується результуюче кодове подання нерівновагового позиційного стеганочисла A' $C'_2 = \varphi_c(N', \Psi^{(1)})$, де φ_c - оператор, що забезпечує побудову двійкового коду C'_2. Зворотне стеганографічне перетворення буде виконуватися за біполярним принципом для авторизованого (за наявності ключа $\Psi^{(2)}$) і неавторизованого користувача (зловмисника) при стандартних умовах.

Перший спосіб використовується неавторизованих користувачів. Таке зворотне перетворення дозволяє достовірно реконструювати елемент $A''(1)$ за формулою: $A(1)'' = f'^{(-1)}(C_2; \Psi^{(1)})$, так, щоб значення кількісної метрика $\varepsilon(A; A(1)'')$ була найменшою: $\varepsilon(A; A(1)'') \to 0$, де $A''(1)$ - елемент, реконструйований при стандартних умовах.

Другий спосіб існує для авторизованого користувача. Тут зворотне функціональне перетворення здійснюється з використанням відкритої службової інформації $\Psi^{(1)}$ і ключа $\Psi^{(2)}$. В даному випадку значення ключа $\Psi^{(2)}$ являє собою заздалегідь відоме значення основи вбудованого елемента так, що б $\Psi^{(2)} \neq \Psi^{(1)}$. Зворотне функціональне перетворення дозволить авторизованому користувачеві безпомилково реконструювати стеганочисло, тобто

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

де $A(2)''$ - НП число з вбудованими даними, отримане при зворотному функціональному перетворенні авторизованим користувачем.

Вилучення вбудованої інформації відбувається без внесення помилок внаслідок застосування оператора вилучення $\varphi_c^{(-1)}$ до реконструйованого НП стеганочисла $A(2)''$ при якому також можливо безпомилкове відновлення числа A'' як елемента вихідного зображення, так що:

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

На рис. 2. відображена схема стеганографічного методу на основі нерівновагового позиційного кодування.

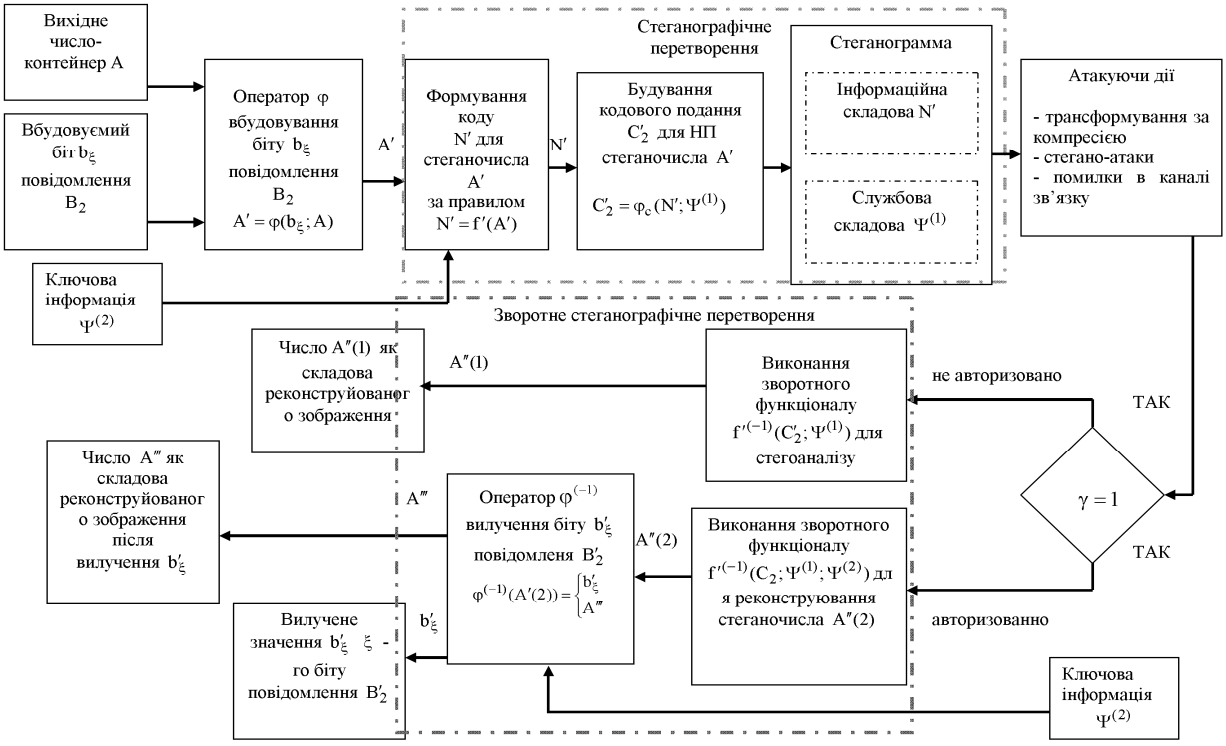

Рис. 2. Схема стеганографічного перетворення на основі нерівновагового позиційного кодування

Пряме стеганографічної перетворення реалізується в три етапи. На першому етапі за допомогою оператора вбудовування φ біт b_ξ приховуваного повідомлення B_2 вбудовується на різну позицію НП числа A.На другому етапі для стеганочисла A' за правилом $f(A')$ формується код N': $N' = f'(A')$. Формування коду відбувається з урахуванням ключової інформації $\Psi^{(2)}$, що припускає під собою підставу вбудованого елемента. На третьому етапі будується результуюче кодове подання C'_2 стеганочисла A'.

Отримана стеганограмма C, що містить в собі інформаційну складову N' і службову складову $\Psi^{(1)}$, піддається атакуючим діям. Зворотне стеганографічної перетворення включає в себе випадок для неавторизованого користувача (стегоаналізу) за умови, що йому відомий зворотний функціонал $f'^{(-1)}$, і авторизованого користувача. Для авторизованого користувача зворотне стеганографічної перетворення відбувається в два етапи.

На першому етапі за правилом $f'^{(-1)}(\bullet)$ і з урахуванням ключової інформації $\Psi^{(2)}$ відбувається реконструкція стеганочисла

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

На другому етапі з реконструйованого стеганочисла $A''(2)$ відбувається вилучення b'_ξ приховуваного повідомлення B_2. В результаті застосування оператора $\varphi^{(-1)}$ вилучення також відбувається реконструкція числа A''', як складового вихідного зображення, що описується виразом

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

Висновки

Запропоновано підхід для підвищення інформаційної безпеки систем спеціального призначення з використанням систем стеганографічного вбудовування інформації в зображення контейнер.

Проведено аналіз недоліків безпосереднього вбудовування на різні позиції просторово-часового представлення зображення-контейнера. Для усунення виявлених недоліків обґрунтовано необхідність застосування функціонального перетворення від числа з вбудованою інформацією. Сформульовані вимоги до синтезованого функціоналу.

Визначено систему властивостей, якому повинен володіти синтезований функціонал, для відповідності вимогам візуальної стійкості до трансформування і атакам. Обґрунтований підхід для функціонального перетворення числа з вбудованою інформацією на основі нерівновагового позиційного кодування.

Список літератури

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

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

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

4. Защита от компьютерного терроризма / А.В. Соколов, О.М. Степанюк. – БВХ-Петрбург : Арлит, 2002. – 496 с.

Надійшла до редколегії 12.02.2015

Рецензент: д-р техн. наук проф. В.В. Бараннік, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

МЕТОД ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ СТЕГАНОГРАФИЧЕСКИХ СИСТЕМ

А.Э. Бекиров

В данной статье предложен подход для повышения информационной безопасности на основе использования методов цифровой стеганографии. Проводится анализ недостатков существующих методов непосредственного встраивания информации на различные позиции пространственно-временного представления изображения-контейнера. Для повышения визуальной устойчивости существующих методов встраивания вводится функционал от числа со встроенной информацией. Вводится система свойств, которыми должен обладать функционал от 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.*

INFORMATION SECURITY METHOD ON THE STEGANOGRAPHY SYSTEMS BASIS

A.E. Bekirov

Approach for increase of information security on the basis of digital steganography methods using is offered in this article. 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.

Keywords: *digital steganography, visual stability, steganogram, algorithms of embedding, nonequilibrium positional number, nonequilibrium positional coding.*