Яковенко Р.С., Мельников О.М.

АНАЛІЗ ОСНОВНИХ МЕТОДІВ СТЕГАНОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В ПРОСТОРОВІЙ ОБЛАСТІ ЗОБРАЖЕННЯ

На сучасному етапі розвитку інформаційних технологій гостро постає проблема як криптографічного захисту інформації (зміна інформації з метою зробити її незрозумілою для осіб, які не мають доступу), так і стеганографічного захисту (способи та методи приховування інформації). Наявність великої кількість відкритих каналів зв'язку спрощує взаємодію між територіально віддаленими користувачами та організаціями, але породжує проблему таємниці передачі самої інформації: як таємницю переданої інформації, так і таємницю самого факту передачі.

Стеганографічне перетворення може відбуватися декількома способами. Загальною рисою є вбудовування інформації в певний об'єкт (контейнер), який передається відкритими каналами зв'язку.

Приховування у просторовій області використовує вбудовування інформації в область первинного зображення. Основною перевагою даного методу є висока швидкість вбудовування, оскільки немає необхідності виконувати складні математичні перетворення зображень.

У [1] виділяють такі основні методи стеганографічних перетворень у просторовій області зображення:

метод найменш значущого біта;

метод псевдовипадкового інтервалу;

метод псевдовипадкової перестановки;

метод заміни палітри;

метод квантування;

метод блокового приховування.

Метод найменш значущого біта полягає у заміні найменшого біта пікселя зображення. Оскільки, даний біт майже не впливає на зображення, можна вважати шумом, тому його можна використовувати для вбудування у зображення інформації. Недоліком даного методу є досить низька місткість контейнера (якщо кожен піксель зображення представлений одним байтом, то місткість контейнера буде 1/8 його загального розміру).

Метод псевдовипадкового інтервалу. Даний метод полягає у випадковому розміщенні бітів повідомлення. У такому випадку відстань між двома сусідніми бітами повідомлення матиме випадковий характер. Місткість контейнера та стійкість до атак сильно залежать від функції розподілення (функції, яка визначає відстань між сусідніми пікселями). Недоліком даного методу є збереження порядку бітів повідомлення в контейнері [1].

Метод псевдовипадкової перестановки [2]. Даний метод виправляє недолік методу псевдовипадкового інтервалу, а саме, збереження послідовності бітів початкового повідомлення. Метод перестановки полягає у використанні генератора псевдовипадкової послідовності індексів пікселів зображення $i_1, i_2, \ldots, i_n$, де відповідно k-біт повідомлення вбудовується в i_k піксель зображення. Як і попередній метод, даний

метод досить сильно залежить від функції розподілення (генератора псевдовипадкової послідовності), яка визначає стійкість до атак. Оскільки у генератора псевдовипадкових чисел обмежений період, то необхідно враховувати можливість повторень індексів, згенерованих генератором.

Метод заміни палітри. Для приховування інформації можна використовувати палітру кольорів зображення [3]. Для зображення формується таблиця кольорів – список (i, λ_i), який визначає відповідність між індексом та його вектором кольору. Кожному пікселю зображення становиться у відповідність певний індекс у таблиці кольорів. Оскільки порядок кольорів у палітрі не є важливим для відтворення загального зображення, конфіденційна інформація може бути прихованою шляхом перестановки кольорів у палітрі. На практиці досить часто зустрічається, що сусідні кольори палітри не обов'язково схожі, тому деякі стеганометоди упорядковують таблицю кольорів таким чином, що сусідні кольори стають подібними. Деякі стеганометоди використовують зменшення загальної кількості кольорів шляхом розмивання зображення [4].

Метод квантування зображення. Метод квантування зображення базується на міжпіксельній залежності. У найпростішому випадку використовується залежність між сусідніми пікселями. Стеганоключ є таблицею, в якій кожному можливому значенню різниці відповідає певний біт. Приклад даної таблиці показано на табл. 1.

Таблиця 1 – Стеганоключ для приховування повідомлення

Залежність	*-3*	*-2*	*-1*	*0*	*1*	*2*	*3*
Біт	*1*	*0*	*1*	*1*	*1*	*0*	*1*

Для приховування біта повідомлення обчислюється різниця та перевіряється на відповідність біту повідомлення. Якщо біт повідомлення не відповідає отриманому значенню з таблицю, та значення залежності замінюється на найближче, яка відповідає даному біту. При цьому корегуються значення інтенсивності пікселів.

Метод блокового приховування. Метод полягає у розбитті контейнера на блоки, що не перетинаються, випадковим чином. Для кожного блоку обчислюється біт парності $b(\Delta_i)$ [1]:

$$b(\Delta_i) = \sum_{j \in \Delta_i}^{mod\ 2} LSB(C_j)$$

У кожному блоці виконується приховування одного біта секретного повідомлення M_i. Якщо біт парності $b(\Delta_i) \neq M_i$, то найменш значимий біт блока Δ_i інвертується, у результаті $b(\Delta_i) = M_i$. Даний метод має малу стійкість проти спотворення контейнера [1]. До основних переваг даного методу можна віднести те, що зміна одного пікселя у блоці майже не призводить до змін статистичної характеристики контейнера та вплив на контейнер можна зменшити шляхом зменшення розміру блока.

У роботі проведено аналіз основних методів приховування повідомлень у просторовій ділянці зображення, а саме методи: найменш значущого біта,

псевдовипадкого інтервалу, заміни палітри, квантування, блокового приховування. Перспективою подальшого дослідження є модифікація методу блокового стеганоперетворення, оскільки даний метод є найбільш стійким до статистичних атак з описаних.

Література

1. Г.Ф. Конахович. Компьютерная стеганография. Теория и практика // Конахович Г.Ф., Пузыренко А.Ю – К: «МК-Пресс», 2006. – 288с.
2. T.Aura, Practical Invisibility in Digital Communication. // Information hiding: First International Workshop “InfoHiding’96”, Springer as Lecture Notes in Computing Science, vol. 1174, 1996 – pp.265-278.
3. A. Wesfeld, A. Pfitzmann, Attacks on Steganographic Systems. Breaking the Steganographic Utilities EzStego, Jsteg, Steganos and S-Tools – and Some Lessons Learned // Proceeding of the Workshop on Information Hiding. 1999 – 16 p.
4. J. Fridrich, A New Steganographic Method For Pallete-Based Image. // Proceedings of the ISBT PISP conference, Savannah, Georgia, Apr. 1998, pp.285-289.