УДК 004.056.5

ЗАСТОСУВАННЯ МЕТОДІВ ОПТИМІЗАЦІЇ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СТЕГАНОГРАФІЧНОГО АЛГОРИТМУ

І. І. Борисенко, Л. В. Скакун

Одеський національний політехнічний університет
Україна, м. Одеса
Boris_enko@ukr.net

Пропонується нова версія стеганографічного алгоритму, який використовує методи оптимізації, для забезпечення більшої в порівнянні з базовим алгоритмом пропускної спроможності каналу прихованого зв'язку разом зі збереженням надійності сприйняття сформованого стеганоповідомлення. Надійність сприйняття забезпечується за рахунок мінімізації впливів вбудованого повідомлення на контейнер-зображення.

Ключові слова: стеганографія, повідомлення, контейнер.

Основною метою використання комп'ютерної стеганографії є приховування повідомлень в цифрових даних (ЦД), таких як мова, зображення, аудіо або відеозапис. ЦД, в які вбудовується повідомлення, носять узагальнену назву – контейнер, результатом такого вбудовування є стеганоконтейнер або стеганографічне повідомлення, яке відкрито пересилається одержувачу каналами загального користування [1]. Будь-який стеганографічний алгоритм характеризується трьома основними властивостями: стійкістю до стеганоаналізу, надійністю сприйняття (стеганоконтейнер візуально не повинен відрізнятися від контейнера), скритою пропускною здатністю. Під скритою пропускною здатністю (СПЗ) розуміють максимальну кількість інформації, яка може бути вкладена в один елемент контейнера [1].

Як правило, вбудовування повідомлення відбувається за рахунок корегування елементів контейнера (в результаті одержуємо стеганоконтейнер), що призводить до зміни його статистичних характеристик. Ці зміни використовуються статистичними методами стеганоаналізу для розпізнавання стеганоконтейнерів. Зрозуміло, що чим менше збурень зазнає контейнер під час вбудовування повідомлення, тим важче стеганоаналітичним методам забезпечити низький рівень похибки при розпізнаванні. В останній час активно ведуться роботи по розробці стеганографічних методів та алгоритмів, які намагаються забезпечити найменш можливий вплив на контейнер як за рахунок вибору елементів контейнера для вбудовування, так і специфіки самого алгоритму [2, 3 та ін.]. Нарівні з методами стеганографії розробляються і методи стеганоаналізу, які враховують принципи роботи алгоритмів таких класів, тому подальший розвиток стеганографії по розробці стійких методів та алгоритмів не втрачає своєї актуальності. У зв’язку з цим в [4] було запропоновано алгоритм організації таємної передачі повідомлень, заснований на знаходженні схожих бітових послідовностей в повідомленні та контейнері, який завдяки малим збуренням контейнера дає хороші показники щодо збереження статистик контейнера після вбудовування повідомлення. Але розроблений в [4] алгоритм, який є привабливим з точки зору його стійкості до статистичного стеганоаналізу, має низьку СПЗ.

В якості повідомлення може виступати будь-яка конфіденційна інформація і, якщо це, скажімо, особисті чи медичні дані, то стеганографічний алгоритм, який вбудовує таку інформацію у контейнер, має забезпечувати велику СПЗ.

Метою роботи є модифікація стеганографічного алгоритму [4] для підвищення його СПЗ поряд із забезпеченням надійності сприйняття стеганоконтейнера.

Контейнер-зображення представляється бінарною матрицею M, біти якої групуються у підмножини M_i (блоки) довжиною m кожна. Біти повідомлення N групуються у підмножини N_i довжиною n, де $m > n$. Вбудовування повідомлення N у контейнер M в базовому алгоритмі [4] проводилося послідовно, тобто біти поточного N_i порівнювалися з бітами відповідного блоку M_i і таким

чином відшукувалося входження N_i в M_i. Якщо б при відшукуванні входження N_i в M_i виявлялося багато точних співпадінь, то можна було б забезпечити дуже високий рівень СПЗ. Нажаль, має місце інша ситуація, аналіз якої [4] показав, що доводиться корегувати біти M_i.

Між СПЗ та рівнем збурень, яких зазнає контейнер після вбудовування повідомлення, завжди повинен існувати розумний компроміс, інакше повідомлення буде легко виявлено стеганоаналітичними методами, або навіть буде порушена надійність сприйняття стеганоконтейнера. Тому було введено параметр *d*, значення якого відповідало кількості бітів, які дозволялося корегувати у разі неспівпадіння N_i з бітами підпослідовності в M_i. Якщо ж бітів для корегування виявлялося більше, ніж *d*, то такий M_i не використовувався або ж корегувалися параметри *m* та *n* (збільшували *m* або (і) зменшували *n*), що зменшувало об'єм інформації, яка передавалася.

В новій версії алгоритму пропонується шукати входження поточного N_i у всіх блоках контейнера. В результаті такого пошуку створюється двовимірний масив стрічками якого є N_i, а стовпцями – M_i, або навпаки, що не суттєво. Елементами масива є кількість бітів K_{ij}, що неспівпадали. Далі розв'язується оптимізаційна задача про призначення кожному N_i блоку M_j для вбудовування по критерію мінімального вибору K_{ij}. Одночасно для кожного вбудованого N_i створюється елемент ключа, який містить номер блоку *j* та номер позиції в блоці, з якої починається вбудована інформація. Якщо блок не використовувався, елементом ключа є 00. Ключ використовується при декодуванні повідомлення.

На основі експерименту можна стверджувати, що нова версія стеганографічного алгоритму має більшу СПЗ, ніж базовий алгоритм, хоча її реальні показники залежать від конкретного повідомлення та вибору значень параметрів *m* та *n*. Для порівняння СПЗ двох алгоритмів – базового та його нової версії — використовувалося середнє значення довжини повідомлення, яке одержувалося наступним чином. В контейнер-зображення вбудовувалися різні бінарні послідовності. В кожному конкретному випадку визначалася довжина повідомлення. Одержані результати усереднювалися для усіх контейнерів, які тестувалися. Так, наприклад, при $m = 48$ і $n = 8$ середня довжина повідомлення для базового алгоритму становила 24 800 бітів, а для його нової версії 25 600.

Процес вбудовування повідомлення в контейнер можна представити як збурення ΔM його матриці M [5]. Можна стверджувати, що надійність сприйняття зберігається, якщо норма матриці збурення $\|\Delta M\|$ буде малою [6]. Враховуючи, яким чином вбудовується повідомлення, а саме – по принципу мінімізації збурень контейнера, можна сподіватися, що $\|\Delta M\|$ буде малою. Обчислення показали, що $\|\Delta M\|$ для обох алгоритмів виявилася приблизно однаковою.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография.— Москва: Солон-Пресс, 2002.

2. Fridrich J., Filler T. Practical methods for minimizing embedding impact in steganography // Proceedings SPIE, Electronic Imaging, Steganography, and Watermarking of Multimedia Contents IX.— 2007.— 6505.— P. 2–3.

3. Hetzl S., Mutzel P. A graph-theoretic approach to steganography// Proc. Communication and Multimedia security.— 2005.— P. 119–128.

4. Борисенко І. І. Методи порівняння послідовностей, як основа нового стеганографічного алгоритму // Труды XV МНПК «Современные информационные и электронные технологии».– Украина, Одесса.– 2014.– Т. 2.– С.159–160.

5. Кобозева А. А. Стеганографический метод, основанный на преобразовании спектра симметричной матрицы // Праці УНДІРТ.– 2006.– № 4 (48).– С. 44–52.

6. Кобозева А. А., Трифонова Е. А. Учет свойств нормального спектрального разложения матрицы контейнера при обеспечении надежности восприятия стегосообщения // Вестник НТУ «ХПИ».– 2007.– № 18.– С. 81–93.

Borisenko I. I., Skakun L. V.

Applying optimization methods to increase steganographic algorithm's efficiency.

The authors propose a new version of the steganographic algorithm using the optimization methods that provides greater bandwidth of covert communications than basic algorithm does, while maintaining the reliability of perception of formed stego-message. Maintaining the perception reliability is provided by minimizing the impact of the embedded message on the cover image.

Keywords: *steganography, messages, container.*