УДК 004.056 (043.2)

Є.В. Ланських[1], С.В. Лада[2], В.М. Зажома[3]

[1]*Черкаський державний технологічний університет, Черкаси*
[2]*Черкаський національний університет ім. Б.Хмельницького, Черкаси*
[3]*Академія пожежної безпеки ім. Героїв Чорнобиля, Черкаси*

ДОСЛІДЖЕННЯ СТАТИСТИЧНИХ ВЛАСТИВОСТЕЙ СПОСОБІВ НУМЕРАЦІЇ БЛОКІВ СТЕГАНОКОНТЕЙНЕРІВ

В статті проведено дослідження можливості застосування операцій матричного кодування, що синтезовані на основі операції суми за модулем, для забезпечення нумерації блоків стеганоконтейнера. Відповідно до отриманих результатів запропоновані нові перспективні способи та рекомендації щодо застосування операцій матричного кодування на основі суми за модулем для нумерації блоків стеганоконтейнера. Проведено дослідження статистичних властивостей розроблених способів шляхом їх тестування за допомогою пакета тестів NIST STS. За результатами тестування сформовано висновки щодо ефективності застосування запропонованих способів нумерації.

Ключові слова: *матричні операції, матричне кодування, стеганоконтейнер, нумерація блоків стеганоконтейнерів.*

Вступ

Постановка проблеми. Сучасний розвиток засобів обчислювальної техніки дав новий поштовх для розвитку сучасних інформаційних технологій, однією з яких є комп'ютерна стеганографія, яка дозволяє передавати повідомлення шляхом вбудовування їх в цифрові дані, які як правило, мають аналогову природу – мова, аудіозаписи, зображення, відео, текстові файли і навіть виконувані файли програм. Вбудовування інформації відбувається шляхом її стеганографічного перетворення [1, 2].

Аналіз останніх досліджень та публікацій. Останні роки характеризуються вдосконаленням існуючих та розробкою нових методів стеганографічного перетвореня [3].

Проте дослідженням щодо використання операцій матричного кодування для перенумерації блоків вбудовування інформації не приділялась достатня увага.

Мета статті – провести дослідження нових способів нумерації блоків для забезпечення рівномірного вбудовування повідомлення в цифровий контейнер.

Основний матеріал

Метою стеганографічного перетворення інформації є вбудовування кожного окремого блоку повідомлення у відповідний підблок цифрового контейнера [4].

Вбудовування блоків повідомлення в контейнер повинно бути рівномірним та рівноймовірним. Для рівномірного вбудовування повідомлення необхідно рівномірне розміщення блоків контейнеру. Рівноймовірне вбудовування повідомлення може бути забезпечене рівноймовірним розміщенням бітів, в які вбудовується інформація.

Приховування повідомлення можливе на рівні похибки отримання зображення для контейнеру, тобто на рівні похибки в найменш значущому біті при аналого-цифровому перетворенні. Повідомлення, що передається, повинно бути замасковане під повномірну та рівно випадкову послідовність найменш значущих бітів контейнеру, що буде розцінюватися як передача зображень низької якості [5].

Можна виділити два шляхи досягнення даної мети:

1. Розбиття повідомлення на фрагменти з наступною перестановкою фрагментів та послідовним вбудовуванням в блоки контейнеру.

2. Перестановка номерів блоків контейнера з послідовним вбудовуванням фрагментів повідомлення в відповідні блоки контейнера.

При необхідності вбудовування великих повідомлень для простоти реалізації алгоритмів вбудовування, як на апаратному так і на програмному рівнях, доцільно створити перетворювач коду з змінною структурою в залежності від ключового елементу контейнера, який буде реалізовувати перестановку номерів елементів контейнера, як для вбудовування повідомлення, так і для його виділення.

Розглянуті в роботі способи нумерації блоків розроблені на основі операцій матричного кодування. Запропоновано використовувати матрицю криптографічного перетворення, що побудована на основі додавання за модулем два. Таку матрицю можна описати моделлю формування хеш-функції:

$$\vec{F} = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n \\ a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{n\,n}x_n \end{pmatrix}, \qquad (1)$$

де $a_{ij} \in [0,1]$; $x_1 ... x_n$ – операнди-розряди відповідно.

Основною вимогою до матриці є те, що матриця повинна бути не виродженою.

Запропоновано наступні способи для нумерації блоків вбудовування інформації на основі моделі (1).

1. ***«Перетворення зростаючої послідовності випадковими матрицями 8*8 байт за модулем 2»***. Початковий контейнер ділиться на необхідну кількість блоків розміром 8, 16, 32, 64, 128 або 256 байт відповідно. Обирається перший стеганоконтейнер, пронумеровується 8, 16, 32, 64, 128 або 256 блоків відповідно. Змінюється матриця і відбувається нумерація наступного стеганоконтейнера. Ця операція виконується для всіх стеганоконтейнерів. Таким чином на кожний стеганоконтейнер формується нова матриця.

2. ***«Перетворення зростаючої послідовності випадковими матрицями 8*8 байт за модулем 2 з наступним додаванням постійного вектора інверсій»***. Даний спосіб нумерації відрізняється від попереднього тим, що над результатами матричного перетворення відбувається криптографічне додавання з маскою інверсій, однаковою для всих номерів блоків стеганоконтейнерів.

3. ***«Перетворення зростаючої послідовності випадковими матрицями 8*8 байт за модулем 2 з наступним додаванням групового вектора інверсій»***. Даний спосіб нумерації відрізняється від попереднього тим, що над результатами матричного перетворення відбувається криптографічне додавання з маскою інверсій, яка є новою для кожного блоку стеганоконтейнера.

4. ***«Перетворення зростаючої послідовності груповим вектором інверсій з наступним перетворенням випадковими матрицями 8*8 байт за модулем 2 з наступним додаванням групового вектора інверсій»***. Даний спосіб нумерації відрізняється від попереднього тим, що перед операцією матричного перетворення відбувається криптографічне додавання з маскою інверсій, яка є новою для кожного блоку стеганоконтейнера.

Для того, щоб визначити ефективність застосування кожного з запропонованих способів нумерації блоків проведемо дослідження статистичних властивостей результатів нумерації блоків стеганоконтейнерів. Для цього використаємо пакет NIST STS, який складається з 15 статистичних тестів, які використовуються для перевірки гіпотези щодо випадковості двійкових послідовностей довільної довжини.

В основі статистичного тесту лежить перевірка деякої нульової гіпотези H_0 такої, що досліджувана послідовність – випадкова. Також передбачена альтернативна гіпотеза H_A, що припускає досліджувану послідовність не випадковою. Таким чином, після перевірки згенерованої послідовності, для кожного тесту робиться висновок щодо відхилення, або прийняття нульової гіпотези H_0.

Для кожного тесту обирається адекватна статистика випадковості, на підставі якої далі відхиляється або приймається гіпотеза H_0. Така статистика, відповідно припущенню на випадковість, володіє деяким розподілом випадкових значень. Теоретично розподіл статистики для нульової гіпотези розраховується із застосуванням математичних методів. Далі із такого зразкового розподілу визначається критичне значення. По проведенні тесту розраховується значення тестової статистики, яке порівнюється із критичним значенням. При перевищенні тестового критичного значення над еталонним, відхиляється нульова гіпотеза випадковості H_0. В іншому випадку робиться висновок про прийняття нульової гіпотези.

Із використанням 15 вбудованих тестів, що входять в пакет NIST STS, розраховується 189 ймовірностей P. Тому результатом тестування є побудова деякого вектору значень обрахованих імовірностей $P = \{P_1, P_2 ..., P_{189}\}$. Ці ймовірності можна розглядати, як окремі результати обчислень тестів.

Для здійснення тестувань були обрані такі параметри: довжина послідовності, що тестується $n = 10^6$ біт; кількість послідовностей, що тестується $m = 100$; рівень значущості; кількість тестів $q = 189$.

Таким чином, обсяг вибірки, що тестується, склав $N = 10^6 \times 100 = 10^8$ біт, кількість тестів (q) для різних довжин $q = 189$. Отже, статистичний портрет ПВП містить 18900 значень імовірності P.

В ідеальному випадку при $m = 100$ і $\alpha = 0,01$ у ході тестування може бути відкинута тільки одна послідовність зі ста, тобто коефіцієнт проходження кожного тесту має складати 99%. Але це занадто жорстке правило. Тому застосовується правило на основі довірчого інтервалу. Нижня межа дорівнює 0,96015.

Статистичні портрети відображають властивості випадковості результатів нумерування блоків стеганоконтейнера на основі запропонованих способів використання матричних операцій.

Оскільки результати тестування першого та другого способів є незадовільними (табл. 1), тому немає сенсу відображати їх статистичні портрети. Статистичні портрети для третього і четвертого запропонованих способів зображено на рис. 1 та 2 відповідно. Зведені результати тестування для запропонованих способів наведено в табл. 1.

Проаналізувавши дані з табл. 1 зведених результатів можна зробити висновок, що найбільш ефективним є четвертий спосіб.

Рис. 1. Статистичний портрет результатів роботи 3 способу нумерації

Рис. 2. Статистичний портрет результатів роботи 4 способу нумерації

Таблиця 1

Зведені результати тестування

Способи реалізації матричних операцій нумерації блоків	Кількість тестів, в яких тестування пройшло		Кількість тестів, в яких тестування не пройшло
	99% послід.	96% послід.	< 96% послід.
1-ий спосіб	7 (3,7%)	7 (3,7%)	182 (96,3%)
2-ий спосіб	27 (14,3%)	27 (14,3%)	162 (85,7%)
3-ий спосіб	44(23,3 %)	133 (70,4%)	56 (29,6%)
4-ий спосіб	151 (79,9%)	189 (100%)	0 (0%)

Отримані результати показують, що запропоновані способи на базі матричного кодування можливо використовувати для вирішення задачі нумерації блоків стеганоконтейнерів.

Висновки

Проведені обчислювальні експерименти дозволяють констатувати, що перетворення на основі операцій матричного кодування можливо використовувати для здійснення нумерації блоків стеганоконтейнерів. Для підвищення криптостійкості алгоритму до статистичного криптоаналізу операцію додавання за модулем 2 доцільно використовувати в якості кінцевої операції для побудови матричних операцій криптографічного перетворення.

Список літератури

1. Стеганография, цифровые водяные знаки и стеганоанализ: моногр. / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин, С.А. Сапожников. – М.: ВК, 2009. – 220 с.

2. Рябко Б.Я. Основы современной криптографии и стеганографии / Б.Я. Рябко, А.Н. Фионов. 2-е изд. – М.: Горячая линия-Телеком, 2013. – 232 с.

3. Безпека комп'ютерних систем. Комп'ютерна стеганографія вчора, сьогодні, завтра. [Електрон. ресурс]. Режим доступу до ресурсу: http://www.kiev-security.org.ua/box/12/80.shtml.

4. Смирнов А.А. Методы и средства компьютерной стеганографии с применением сложных дискретных сигналов для защиты информации в компьютерных системах и сетях: моногр. / А.А. Смирнов – К.: Изд. «КОД», 2012. – 350 с.

5. Юдин О.К. Захист інформації в мережах передачі даних / О.К. Юдин, О.Г. Корченко, Г.Ф. Конахович. – К. Вид-во ТОВ «НВП-ІНТЕРСЕРВІС», 2009. – 716 с.

Надійшла до редколегії 14.06.2014

Рецензент: д-р техн. наук, проф. І.В. Шостак, Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», Харків.

ИССЛЕДОВАНИЕ СТАТИСТИЧЕСКИХ СВОЙСТВ СПОСОБОВ НУМЕРАЦИИ БЛОКОВ СТЕГАНОКОНТЕЙНЕРОВ

Е.В. Ланских, С.В. Лада, В.М. Зажома

В статье проведено исследование возможности использования операций матричного кодирования, синтезированных на основе операций суммы по модулю, для обеспечения нумерации блоков стеганоконтейнера. В соответствие с полученными результатами предложены новые перспективные способы и рекомендации касательно использования операций матричного кодирования на основании суммы по модулю для нумерации блоков стеганоконтейнера. Проведено исследование статистических свойств разработанных способов путем их тестирования с помощью пакета тестов NIST STS. По результатам тестирования сформированы выводы по эффективности использования предложенных способов нумерации.

Ключевые слова: *матричные операции, матричное кодирование, стеганоконтейнер, нумерация блоков стеганоконтейнеров.*

INVESTIGATING STATISTIC PROPERTIES OF THE METHODS OF NUMBERING STEGANOCONTAINER BLOCKS

Y.V. Lanskykh, S.V. Lada, V.M. Zazhoma

The paper investigated the possibility of using matrix encoding operations synthesized and based on the sum of modulus operations, for providing the numbering of steganocontainer blocks. In accordance with the results, new promising methods and recommendations are offered regarding to the use of matrix encoding based on the sum of modulus for numbering the steganocontainer blocks. The study of the statistic properties, developed methods by testing them with the help of test package NIST STS, is carried out. Conclusions on the effectiveness of the proposed methods of numbering are formed according to test results.

Keywords: *matrix operations, matrix encoding, steganocontainer, numbering of steganocontainer blocks.*