DOI 10.15276/imms.v10.no1-2.55
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 10 (2020), No. 1-2, pp. 55-60

МОДИФІКАЦІЯ МЕТОДУ ХЕШ-СТЕГАНОГРАФІЇ, ЗАСНОВАНОГО НА ПЕРЕДАЧІ ПОСЛІДОВНОСТІ ЦИФРОВИХ ЗОБРАЖЕНЬ

В.В. Зоріло, О.Ю. Лебедєва, М.В. Бохонько

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: whiteswanhelena@gmail.com

Захист електронної інформації криптографічними та стеганографічними методами, а також їх комбінацією сьогодні є дуже затребуваним. Проте новий вид стеганографії – хеш-стеганографія, принципово відрізняється від класичної стеганографії тим, що не потрібно вбудовувати повідомлення в контейнер, не потрібно хвилюватись про кількість інформації, яку можна передати в одному контейнері, не порушивши візуальну стійкість зображення. Певна послідовність звичайних цифрових зображень – це і є повідомлення. Метою даної роботи є підвищення ефективності передачі секретного повідомлення шляхом модифікації метода хеш-стеганографії. Раніше алгоритми отримання хеш-функцій цифрових зображень не використовували для передачі повідомлень, проте вони знайшли своє застосування в хеш-стеганографії. В даній роботі виконано порівняння двох алгоритмів отримання хеш-кодів та запропоновано метод їх застосування для перетворення текстового повідомлення на послідовність цифрових зображень. Саме певний порядок файлів, що передаються, і є вирішальним при розшифруванні повідомлення. Символам повідомлення ставиться у відповідність частина хеш-коду цифрового зображення. Таким чином утворюється необхідна комбінація файлів, кількість яких дорівнює кількості символів повідомлення. В роботі проведено порівняльний аналіз двох алгоритмів методу. Отримані результати підтвердили ефективність використання алгоритму отримання хеш-кодів, заснованого на аналізі коефіцієнтів ДКТ цифрового зображення. Даний алгоритм робить метод стійким до атак стисненням, зміною яскравості та контрастності, масштабуванням та обертанням.

Ключові слова: хеш-стеганографія, цифрове зображення, хеш-код.

Вступ

Використання різних технологій приховування процесу інформаційної взаємодії з метою приховування інформації при її подальшої передачі по відкритих каналах зв'язку є не новим в нинішніх реаліях повсякденного життя людини. Для забезпечення скритності повідомлення, що міститься в носії (контейнері), використовуються різні стеганографічні методи. При цьому поряд з конфіденційністю набуває все більшої актуальності забезпечення цілісності переданих по незахищеним каналам даних. В якості основного методу захисту інформації від нелегітимних користувачів при організації інформаційної взаємодії застосовується криптографічний захист, який має високу ефективність через гарантовану стійкість сучасних систем шифрування [1]. Також сучасні методи захисту інформації неможливо уявити без стеганографічних методів, які, на відміну від криптографічних, приховують сам факт передачі повідомлення. Однак, коли ми вбудовуємо повідомлення в стеганографічні контейнери, завжди є ризик модифікації чи втрати повідомлення в результаті атаки. Також важливою проблемою в даній області є пропускна здатність, тобто кількість інформації, яку можна непомітно вбудувати в контейнер. Для того, аби уникнути цих проблем, винайшли альтернативний вид стеганографії – хеш-стеганографія. В роботі [2] запропоновано не вбудовувати в зображення-контейнери інформацію, а використовувати послідовність зображень, а саме безпосередньо хеш-код зображень

для побудови секретного повідомлення. Тобто хеш-стеганографія заснована на тому, що певна послідовність цифрових сигналів, зокрема цифрових зображень, і є повідомленням. Встановлюється відповідність між хеш-кодами зображень та певними символами, які в визначеній послідовності формують секретне повідомлення. В роботі [3] запропоновано метод хеш-стеганографії, заснований на використанні цифрових зображень та їх хеш-кодів для передачі секретного повідомлення. Дана стаття є продовженням попередньої роботи. В ній описано доповнений хеш-стеганографічний метод, заснований на передачі послідовності цифрових зображень.

Мета роботи

Метою роботи є підвищення ефективності передачі секретного повідомлення шляхом модифікації метода хеш-стеганографії.

Матеріали та методи

Модифікація методу, описаного в [3], полягає в наступному. Отримання хеш-коду пропонується виконувати алгоритмом Perceptual Hash (далі pHash) [4], який має певні переваги перед алгоритмом Average Hash (далі aHash), використаним в [3], а саме стійкість хешкоду до певних афінних перетворень за рахунок використання ДКП.

У зображеннях є відповідність між частотним спектром та інформаційною наповненістю. Високі частоти зображення відповідають деталям, контурам, зміні функції яскравості пікселів тощо. Низькі частоти відповідають фоновим частинам, несуть основну інформацію. Високі частоти чутливі до багатьох атак: стиснення, зміна чіткості зображення розмиттям чи підвищенням різкості тощо. Низькі частоти більш стійкі до подібних змін. Логічно використовувати низькочастотну складову сигналу для передачі секретного повідомлення. Тобто необхідно виконати певні перетворення цифрового зображення, перш ніж генерувати його хеш-код.

Найшвидший спосіб видалити високі частоти та деталі – зменшити зображення. Алгоритм aHash має одним з кроків зменшення зображення до розмірів 8×8, щоб загалом було 64 пікселі. Збереження пропорцій не є важливим у даному випадку. Таким чином, хеш буде відповідати будь-яким варіаціям зображення, незалежно від масштабу або співвідношення сторін. Далі рисунок розміром 8×8 необхідно перевести у градації сірого. Це змінює хеш із 64 пікселів (64 червоних, 64 зелених та 64 синіх) на 64 загальні кольори. Потім обчислюємо середнє значення N для 64 кольорів. Перетворюємо зображення в бінарну послідовність наступним чином. Порівнюємо значення кожного пікселя зображення із значенням N. Якщо значення пікселя менше за N, то ставимо йому у відповідність значення 0, інакше – 1. Формуємо вектор із значень 0 та 1. Отриману послідовність шифруємо за допомогою шифру MD5. Даний алгоритм генерує хешкоди, стійкі до масштабування та зміни співвідношення сторін, до стиснення зображення, проте нестійкий до таких афінних перетворень як повороти ЦЗ та корекції яскравості кольорів.

Розглянемо перцептивний алгоритм (pHash). За аналогією з попереднім алгоритмом зменшуємо розмір зображення до 32×32. Переходимо до зображення в градаціях сірого. Обчислюємо ДКП. Для роботи нам потрібні низькі частоти, як було зазначено вище, тому в даному алгоритмі використовують коефіцієнти ДКП верхнього лівого блоку 8×8. Вони відповідають найнижчим частотам зображення. Обчислюємо середнє значення коефіцієнтів ДКП за виключенням першого коефіцієнта, оскільки він може значно відрізнятися від інших значень і буде відкидати середнє значення. Поставимо у відповідність коефіцієнтам ДКП бінарну послідовність, де 0 відповідає

коефіцієнтам, значення яких менше за середнє, 1 – більше. Переводимо 64-бітову послідовність у 64-бітове ціле число.

Основні етапи модифікованого методу хеш-стеганографії представлено далі.

На першому етапі створюються бази даних (далі БД) хеш-кодів зображень. Для коректної роботи даного методу необхідна велика кількість унікальних зображень. На даному етапі розраховуються хеш-коди усіх зображень за допомогою вищезазначеної хеш-функції (рис.1). Будемо використовувати перші два символи хеш-коду.

```
e84014ff8666378de4f997e4536950f3
aed21eb87010e8dcd8f77d5ef2b3b64b
388bb38e38db9d3474d076e92154e178
bf0c959a017a46abe942dc47a2f96843
e0a952358b03def495fe558da26f208b
a76b210b02bc63050a0943cd25edc2ed
ec1ad6716c85a93c3164223ba978f2e1
cf097b964ab7ca0b3d48b19f64e1eb94
0f8c3ecb62a71ee6a4f3ac862acb180a
2eb87b2767e836e9792c0dfcac762212
6ebec9533947729d4fd61d8954df2c9c
```

Рис. 1. Хеш-коди деяких зображень

Зображення підбираються таким чином, щоб одному символу повідомлення відповідали чотири зображення. Символи повідомлення кодуються в системі ASCII. Код символу повинен відповідати першим двом символам хеш-кодів зображень (рис. 2).

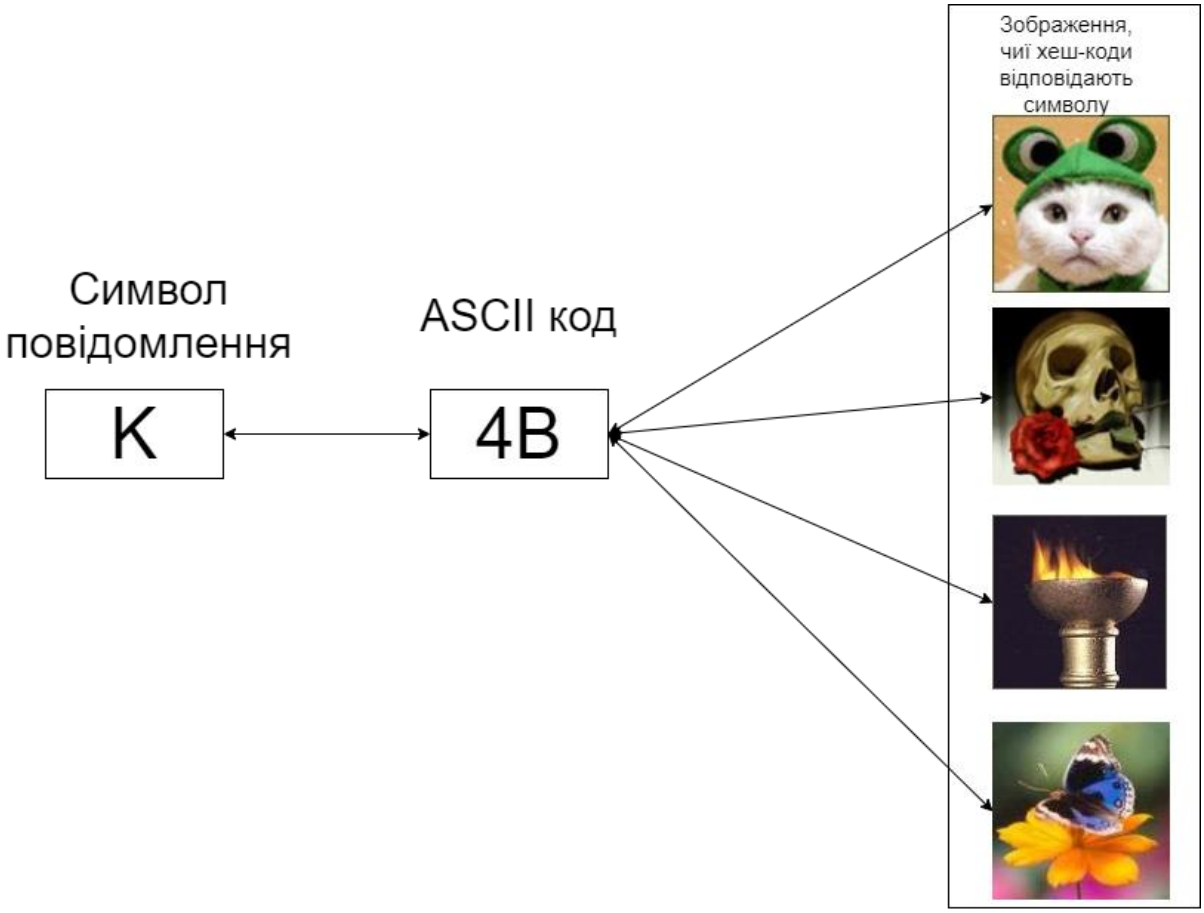

Рис. 2. Схема відповідності «символ-зображення»

На другому етапі вводимо повідомлення для передачі. Переводимо повідомлення в систему ASCII та розбиваємо на рівні частини по 2 символи [5]. Для кожного символу повідомлення відбираємо відповідне зображення перше в черзі. Якщо зображення було використано раніше, беремо наступне зображення у черзі. Якщо всі зображення були використані, цикл починається з початку.

На третьому етапі отримуємо послідовність зображень, яка є контейнером стеганоповідомлення та готова для відправлення.

Приклад результату роботи метода показано на рисунку 3, де закодовано повідомлення «Bad company».

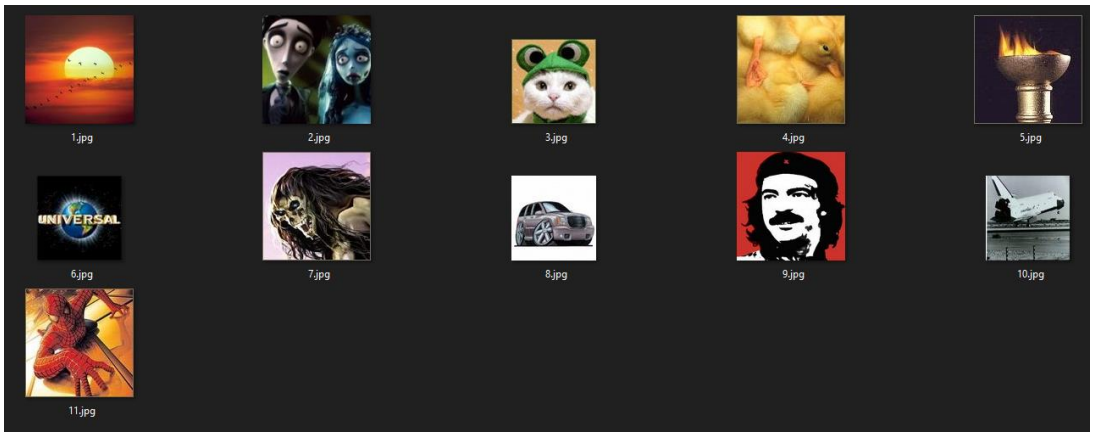

Рис. 3. Відібрані зображення, які шифрують словосполучення «Bad company»

Результати та обговорення. Одержувач після отримання зображень зберігає їх у тому ж порядку, генерує їх хеш-коди, з перших двох символів кожного хеш-коду формує ASCII-код. Далі одержувач переводить ASCII код в символи латинського алфавіту і отримує початковий текст повідомлення.

Основна ідея методу полягає у використанні перцептивних хеш-функцій aHash та pHash, за допомогою яких отримуються стійкі хеш-коди зображень до різних видів атак, таких як: масштабування, стиснення, зміна яскравості або контрасту. Порівняємо ефективність відновлення повідомлень, переданих подібним шляхом (табл.1).

Таблиця 1.

Порівняння ефективності алгоритмів методу хеш-стеганографії

Алгоритм / Вид атаки	aHash	pHash
Обертання (не більше 30°)	87	94
Зміна контрастності	85	95
Масштабування	92	97
Стиснення JPG	96	96
Зміна яскравості	91	95

Як бачимо з таблиці, використання pHash дало кращі результати в порівнянні з aHash, що дозволило підвищити ефективність передачі секретних повідомлень.

Висновки

В результаті даної роботи виконано модифікацію методу хеш-стеганографії. Отримані результати обчислювального експерименту показали, що використання

алгоритму pHash, заснованого на ДКП, дає кращі результати відновлення повідомлення з послідовності цифрових зображень в порівнянні з алгоритмом aHash, який працює зі значеннями яскравості пікселів напряму.

Список літератури

1. Pfitzmann B. Information hiding terminology, information hiding. *First international workshop of lecture notes in computer science*. Berlin: Springer-Verlag, 1996. P. 347-350.
2. Shin N. One-Time Hash Steganography. Heidelberg: Springer-Verlag, 2000. P.17-28.
3. Бохонько М.В, Зоріло В.В. Модифікація методу хеш-стеганографії. VII *Міжнародна науково-практична інтернет-конференція «Сучасний рух науки», 6-7 червня 2019 р*. Дніпро, 2019. С.605-608.
4. Looks Like It. URL: www.hackerfactor.com/blog/index.php?/archives/432-Looks-Like-It.html.
5. ASCII Code – The extended ASCII table. URL: www.ascii-code.com.

МОДИФИКАЦИЯ МЕТОДА ХЕШ-СТЕГАНОГРАФИИ, ОСНОВАННОГО НА ПЕРЕДАЧЕ ПОСЛЕДОВАТЕЛЬНОСТИ ЦИФРОВЫХ ИЗОБРАЖЕНИЙ

В.В. Зорило, Е.Ю. Лебедева, М.В. Бохонько

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: whiteswanhelena@gmail.com

Защита электронной информации криптографическими и стеганографическими методами, а также их комбинацией сегодня является очень востребованной. Однако новый вид стеганографии – хэш-стеганография, принципиально отличается от классической стеганографии тем, что не нужно встраивать сообщение в контейнер, не нужно волноваться о количестве информации, которую можно передать в одном контейнере, не нарушив визуальную устойчивость изображения. Определенная последовательность обычных цифровых изображений – это и есть сообщение. Целью данной работы является повышение эффективности передачи секретного сообщения путем модификации метода хеш-стеганографии. Ранее алгоритмы получения хэш-функций цифровых изображений не использовались для передачи сообщений, однако они нашли свое применение в хеш-стеганографии. В данной работе выполнено сравнение двух алгоритмов получения хэш-кодов и предложен метод их применения для преобразования текстового сообщения в последовательность цифровых изображений. Именно определенный порядок передаваемых файлов и является решающим при расшифровке сообщения. Символам сообщения ставится в соответствие часть хэш-кода цифрового изображения. Таким образом образуется необходимая комбинация файлов, количество которых равно количеству символов сообщения. В работе проведен сравнительный анализ двух алгоритмов метода. Полученные результаты подтвердили эффективность использования алгоритма получения хэш-кодов, основанного на анализе коэффициентов ДКП цифрового изображения. Данный алгоритм делает метод устойчивым к атакам сжатием, изменением яркости и контрастности, масштабированием и вращением.

Ключевые слова: хеш-стеганография, цифровое изображение, хеш-код.

MODIFICATION OF THE HASH-STEGANOGRAPHY METHOD BASED ON THE TRANSFER OF A SEQUENCE OF DIGITAL IMAGES

V.V. Zorilo, O.Yu. Lebedeva, M.V. Bokhonko

Odessa National Polytechnic University,
1, Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: whiteswanhelena@gmail.com

The protection of electronic information by cryptographic and steganographic methods, as well as their combination, is in great demand today. However, the new type of steganography – hash-steganography, fundamentally differs from classical steganography in that there is no need to embed messages in a container, no need to worry about the amount of information that can be transmitted in one container without compromising the visual stability of the image. A certain sequence of ordinary digital images is a message. The purpose of this work is to increase the efficiency of transmitting a secret message by modifying the hash-method of steganography. Previously, algorithms for obtaining hash functions of digital images have not been used to transmit messages, but they have found their application in hash-steganography. This paper compares two algorithms for obtaining hash codes and suggests a method of their application for transforming a text message into a sequence of digital images. It is a certain order of files transferred that is decisive in the decryption of a message. The symbols of the message are put in correspondence with the part of the hash code of the digital image. Thus, the necessary combination of files is formed, the number of which is equal to the number of symbols in the message. A comparative analysis of the two algorithms of the method has been performed. The results obtained have confirmed the effectiveness of the hash code algorithm based on the analysis of digital image DCT coefficients. This algorithm makes the method resistant to attack by compression, changing brightness and contrast, magnification and rotation.

Keywords: hash-steganography, digital image, hash-code.