УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 9 (2019), No. 1-2, pp. 69-76

МОДИФІКАЦІЯ АЛГОРИТМУ ХЕШ-СТЕГАНОГРАФІЇ

В.В. Зоріло, М.В. Бохонько, А.І. Казаков

Одеський національний політехнічний університет
просп. Шевченко, 1, Одесса, 65044, Україна; e-mail: mishabahus28@gmail.com

Інформація, яка передається каналами зв'язку, піддається різноманітним загрозам, таким, як викриття, спотворення та знищення. Одним із можливих рішень проблеми загрози викриття є використання стеганографічних методів, які, в свою чергу, мають свої обмеження за областю застосування. Стеганографія передбачає вбудовування секретного повідомлення у стеганографічний контейнер (наприклад, цифрове зображення) так, щоб не порушувати стійкість візуального сприйняття контейнера. Одною з основних вимог стеганографічного методу є його стійкість до різноманітних видів атак. Сучасний напрям стеганографії, хеш-стеганографія, базується на обчисленні хеш-коду цифрових зображень та повідомлення, що передається, та подальшому використанні отриманих хеш-кодів для передачі секретного повідомлення. Зазвичай більшість атак на цифрові зображення складають небезпеку переважно для високих частот сигналу, в результаті чого хеш-код цифрового зображення також зазнаватиме змін, що може призвести до часткової або повної втрати стеганографічного повідомлення. Більшість сучасних методів отримання хеш-коду цифрового зображення засновані на використані високих частот, що робить методи хеш-стеганографії вразливими до атак. Метою роботи є підвищення ефективності алгоритму хеш-стеганографії шляхом його модифікації за допомогою перцептивних хеш-алгоритмів. Проведено аналіз існуючих перцептивних хеш-алгоритмів для обчислення хеш-коду зображення. Виконано модифікацію алгоритму хеш-стеганографії. Модифікований алгоритм заснований на використанні перцептивного хеш-алгоритму Simple Hash. Проведено аналіз ефективності модифікованого алгоритму, який показав, що модифікація забезпечує підвищення стійкості стеганоповідомлення до різних атак в порівнянні з оригіналом.

Ключові слова: стеганографія, хеш-стеганографія, перцептивний хеш-алгоритм, вбудовування додаткової інформації.

Вступ

Як відомо, для захисту даних найчастіше використовують криптографію, але наявність зашифрованого повідомлення привертає до себе увагу і створює інтерес до злому переданого повідомлення. Для того, щоб цього уникнути, використовують криптографію спільно зі стеганографією. Стеганографія представляє собою вбудовування секретного повідомлення із подальшим його відновленням у стеганографічний контейнер (наприклад, цифрове зображення) так, щоб не порушувати стійкість візуального сприйняття контейнера. Стеганографія приховує сам факт передачі інформації. Наприклад, передача повідомлення відбувається під виглядом передачі зображення у форматі JPEG. Одною з основних вимог до стеганографічного методу є його стійкість до різноманітних видів атак. Сучасний напрям стеганографії – хеш-стеганографія, базується на обчисленні хеш-коду цифрових зображень та повідомлення, що передається, і в подальшому використанні отриманих хеш-кодів для передачі секретного повідомлення. Зазвичай більшість атак на цифрові зображення складають «небезпеку» переважно для високих частот, в результаті чого хеш-код цифрового зображення також зазнаватиме змін, що може призвести до часткової або повної втрати стеганографічного повідомлення. Більшість сучасних методів отримання

хеш-коду цифрового зображення засновані на використанні високих частот, що робить методи хеш-стеганографії вразливими до атак.

Мета роботи

Метою роботи є підвищення ефективності алгоритму хеш-стеганографії шляхом його модифікації за допомогою перцептивних хеш-алгоритмів.

Основна частина

Нині часто при шифруванні та приховуванні секретних повідомлень стеганографія та криптографія використовуються разом: інформацію, яку передають, шифрують спочатку стійким криптографічним методом; далі отримане повідомлення вбудовують в контейнер (зображення) [1]. Як правило, при цьому в зображені з'являються зміни, непомітні для людського ока. І для шифрування, і для дешифрування використовують секретний ключ, який передають захищеним каналом зв'язку.

Проте, хеш-стеганографія використовує інший принцип. Щоб уникнути зайвої уваги зі сторони зловмисника, не обов'язково вбудовувати повідомлення у зображення, змінюючи його. Головний принцип хеш-стеганографії полягає у тому, що послідовність зображень, що передаються, і є повідомленням [2].

Для того, щоб передати секретне повідомлення, необхідно обчислити його хеш-код і передавати дане повідомлення у вигляді послідовності зображень, хеш-коди яких певним чином частково співпадають з хеш-кодом повідомлення. Розглянемо детальніше основні кроки такого виду шифрування.

Для ефективного шифрування повідомлення для початку необхідно створити велику базу цифрових зображень. Далі за допомогою криптографічної хеш-функції, яка задовольняє властивості рівноймовірності (наприклад, MD5), розраховуємо хеш-код усіх зображень, дані заносимо в таблицю. Припустимо, що необхідно передати повідомлення «morior» в шістнадцятирічному вигляді: 56585B52585B. Тоді основні кроки алгоритму хеш-стеганографічного шифрування будуть наступні. Дане повідомлення розділяємо на біграми: 56 58 5B 52 58 5B. Отримані біграми будемо називати словами (у загальному випадку слова можуть мати більшу довжину). В прикладі, що розглядається, є шість слів. Кожному слову ставиться у відповідність зображення, перші n символів якого співпадають зі словом (n дорівнює довжині слова). В результаті отримаємо послідовність зображень, які представляють собою повідомлення, що передається.

Такий спосіб передачі повідомлень досить простий, але він не є надійним з наступних причин. Якщо при передачі буде проведено атаку на цифрові зображення (які, нагадаємо, в певній послідовності і є повідомленням), то хеш-код зображень буде змінено, і повідомлення буде втрачено.

Для вирішення цієї проблеми в даній роботі запропоновано наступний підхід. Підвищити надійність шифрування та стійкість до атак можна за допомогою використання перцептивного хеш-алгоритму. Особливість усіх перцептивних хеш-алгоритмів полягає у тому, що при різних перетвореннях зображення, наприклад, при зміні розміру, зміні співвідношення сторін, незначних змінах яскравості, контрастності тощо, хеш-код зображення не змінюється. Розглянемо деякі перцептивні хеш-алгоритми.

Ідея перцептивного хеш-алгоритму Simple Hash полягає у відображенні середнього значення низьких частот [3]. У зображеннях високі частоти забезпечують деталізацію, а низькі – показують структуру. Тому для побудови такої хеш-функції, яка

для схожих збережень видаватиме близький хеш-код, доцільно «позбутися» високих частот.

В роботі [4] описано алгоритм Discrete Cosine Transform Based Hash, ідея якого полягає у розрахунку середнього значення за допомогою дискретного косинусного перетворення для невраховування високих частот з сигналу-зображення.

Суть алгоритму Radial Variance Based Hash полягає в побудові променевого вектору дисперсії на основі перетворення Радону [5]. Потім до променевого вектора дисперсії застосовують дискретне косинусне перетворення і обчислюють хеш-код. Перетворення Радону стійке до обробки зображень за допомогою різних маніпуляцій (наприклад, стиснення) і геометричних перетворень (наприклад, поворотів).

Алгоритм MarrHildreth Operator Based Hash також зарекомендував себе як стійкий до атак [6]. Оператор Марра-Хілдрет дозволяє визначати границі на зображенні. Взагалі кажучи, границю на зображенні можна визначити як край або контур, що відокремлює сусідні частини зображення, які мають порівняно відмінні характеристики відповідно до деяких особливостей.

Цими особливостями можуть бути колір або текстура, але частіше за все використовують сіру градацію кольору зображення (яскравість). Результатом визначення меж є карта кордонів. Карта кордонів описує класифікацію меж для кожного пікселя зображення. Якщо границю визначати як різку зміну яскравості, то для їх знаходження можна використовувати похідні або градієнт.

Для досягнення поставленої в роботі мети було обрано перцептивний хеш-алгоритм Simple Hash – він легкий в реалізації та відносно швидкий у роботі. Основні кроки перцептивного алгоритму Simple Hash наведені нижче.

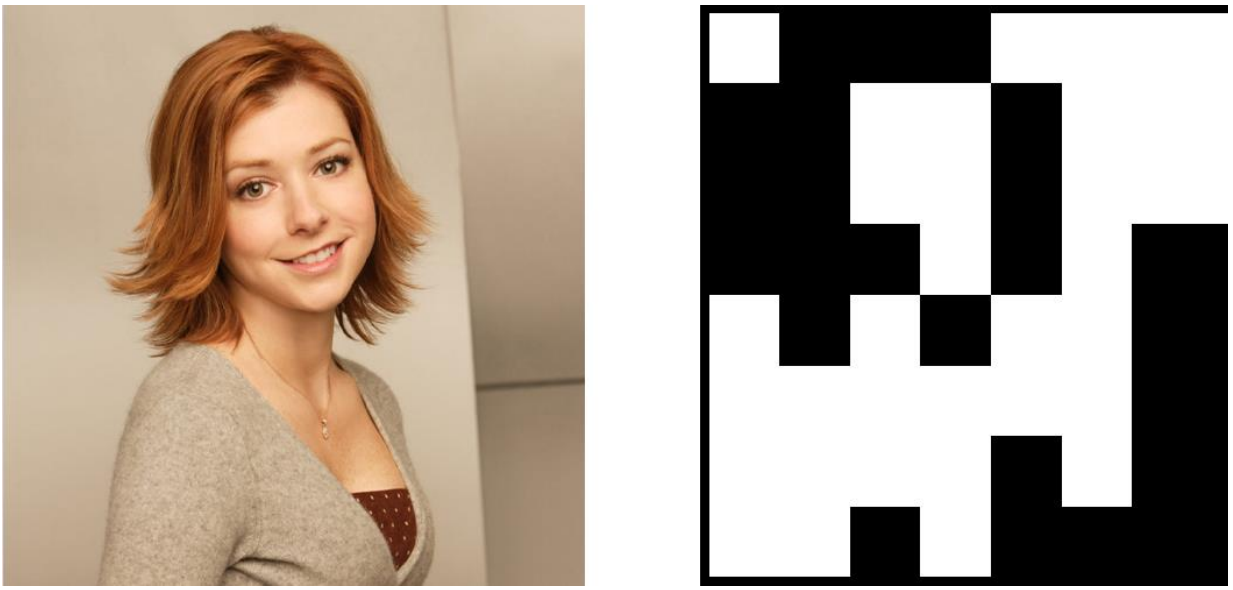
Перший крок – зменшення розміру цифрового зображення шляхом масштабування його до розміру 8×8 пікселів незалежно від початкового розміру. Найшвидший спосіб позбутися від високих частот – зменшити зображення шляхом масштабування. Завдяки цьому ще більше спрощуємо наступні етапи, не втрачаючи занадто багато структурної інформації зображення, а також отримуємо деяку міру інваріантності масштабу. На другому кроці необхідно прибрати колір, тобто перевести вхідне зображення у відтінки сірого (рис. 1).

а б в

Рис. 1. Зменшення розмірів та зміна кольорового режиму зображення: а – оригінальне зображення; б – зменшене зображення; в – зображення у градаціях сірого

Цей крок значно підвищує швидкість роботи алгоритму за рахунок скорочення обсягу інформації, яку потрібно обробляти на більш пізніх етапах. Після цього необхідно знайти середнє значення пікселів. Робимо це шляхом підсумовування всіх значень нашого зображення і ділення результату на 64.

На наступному етапі необхідно побудувати ланцюжок бітів. Для кожного пікселя зображення робиться наступна заміна. Якщо значення пікселю більше середнього, то замість значення кольору ставимо 1. Аналогічно, якщо значення пікселю менше середнього – ставимо 0 (рис. 2).



а б

Рис. 2. Приклад кінцевого результату масштабування та представлення в бінарному вигляді сірого початкового зображення: а – початкове зображення; б – отриманий «відбиток»

Записуємо значення отриманого бітового зображення у певній послідовності, в результаті чого отримаємо значення довжиною 64 біт. Послідовність зчитування не має значення, але зазвичай біти записуються зліва направо, зверху вниз. Після виконання усіх кроків останнім етапом є побудова хеш-коду. За допомогою хеш-функції (наприклад, SHA-3 [7]) розрахуємо хеш-код бітової послідовності, отриманої на попередньому кроці.

Етапи модифікованого алгоритму хеш-стеганографії полягають в наступному.

Для кожного зображення обчислюємо значення хеш-коду за допомогою перцептивного алгоритму Simple Hash (рис. 3). Отримані значення хеш-коду запишемо в текстовий файл, який будемо зберігати для подальшого використання при кожному шифруванні повідомлення.

Кожен окремо взятий символ повідомлення переводимо в систему ASCII і порівнюємо кожну пару значень з першими двома символами хеш-кодів зображень. В результаті отримаємо набір зображень. Виконавши перераховані кроки з усіма символами повідомлення, отримаємо набір зображень (відповідно до кількості символів повідомлення), які слід відправляти одержувачу в певно визначеному порядку, інакше сенс повідомлення загубиться.

Приклад зашифрованого таким чином повідомлення (рис. 4).

Одержувач, отримавши зображення, записує у рядок перші два символи хеш-кодів, в результаті чого отримує ASCII-код. Далі необхідно перевести ASCII-код в текст, який і буде повідомленням.

Описаний спосіб шифрування не позбавлений недоліків, проте має і певні переваги. До недоліків можна віднести наступні фактори. Створення нової або оновлення існуючої бібліотеки зображень займає великий проміжок часу.

Масштабування зображень, перехід до градацій сірого, обчислення середнього арифметичного значення яскравості пікселів у градаціях сірого та побудова бітової

послідовності для зображення – доволі громіздкий процес для середніх обчислювальних машин.

```
e84014ff8666378de4f997e4536950f3
aed21eb87010e8dcd8f77d5ef2b3b64b
388bb38e38db9d3474d076e92154e178
bf0c959a017a46abe942dc47a2f96843
e0a952358b03def495fe558da26f208b
a76b210b02bc63050a0943cd25edc2ed
ec1ad6716c85a93c3164223ba978f2e1
cf097b964ab7ca0b3d48b19f64e1eb94
0f8c3ecb62a71ee6a4f3ac862acb180a
2eb87b2767e836e9792c0dfcac762212
6ebec9533947729d4fd61d8954df2c9c
65d7d095eecca3ab197792c07dbfd481
3198feb4dbd2fa68ae318f9b7df41def
041056ba10bfc48a3119716b1e63417c
d1b3346e2d5cee3df607a6c40fe59c7a
50efb5183b6cfa2c75f63e17a0ac936d
804e46f6d91716e1253e3aa679b0d630
de5e9e8f27e96e8bbd2e1ceed06c29b4
```

Рис. 3. Хеш-коди декількох зображень

Рис. 4. Відібрані зображення, які шифрують повідомлення «Bad company»

Проте, незручності це викликатиме лише при першому запуску самого програмного продукту. Усі наступні звернення до даного методу шифрування проходитимуть значно швидше саме через те, що буде сформовано файл для зберігання отриманих хеш-кодів для усіх зображень, що їх використовують при передачі секретного повідомлення. Другим недоліком є те, що, як було зазначено вище, необхідна велика бібліотека зображень. Для експериментів, описаних у даній роботі, було використано 1500 унікальних зображень, чого виявилося достатньо при розбитті повідомлення на біграми.

До переваг даного алгоритму можна віднести наступне. Хеш-коди зображень мають високу стійкість до різноманітних видів атак на зображення – масштабування, стиснення, корекція яскравості та контрастності зображення. Зазвичай повідомлення вбудовується в цифрове зображення, тим саме пошкоджуючи високі частоти зображення. Якщо при передачі на зображення буде проведена атака, то стегано-повідомлення буде пошкоджене або взагалі втрачене. Схему кодування представлено на рисунку 5.

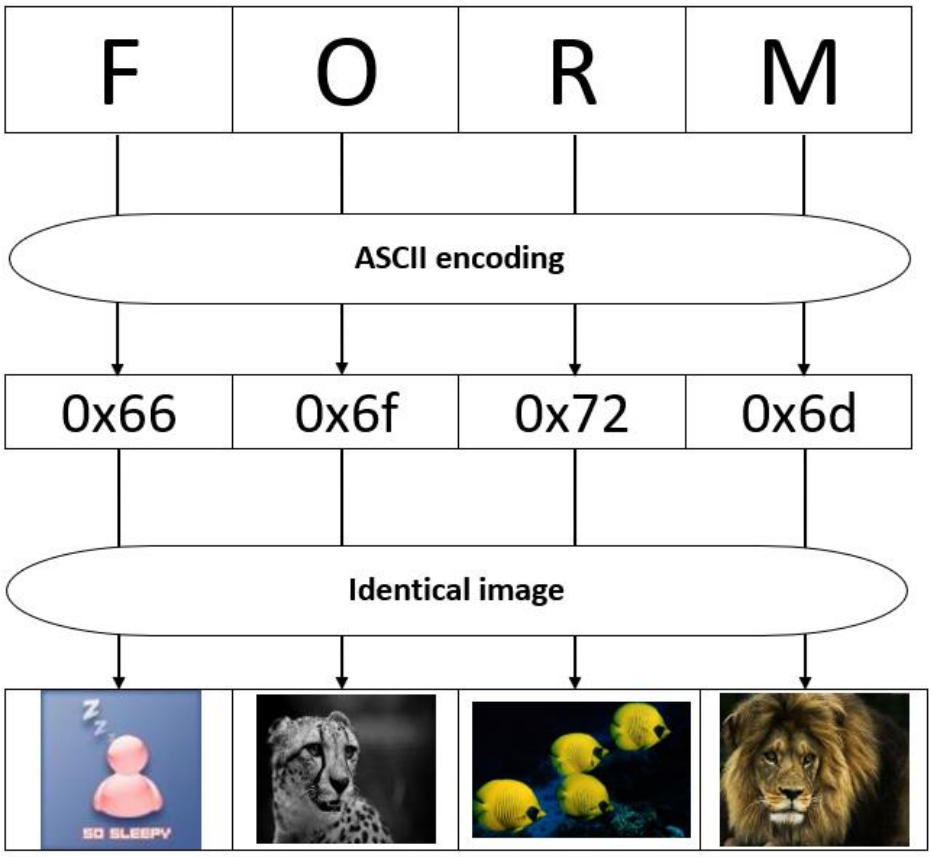


Рис. 5. Схема кодування повідомлення

Декодування відбувається у зворотньому порядку. Проведено також аналіз ефективності даного алгоритму кодування при застосуванні стеганографічних атак на послідовність цифрових зображень. Види атак та результати аналізу представлено у таблиці 1. До повідомлень у вигляді зображень було застосовано масштабування, корекцію яскравості та стиснення.

Таблиця 1.

Аналіз ефективності алгоритму при застосуванні стеганографічних атак

Стеганографічна атака	Масштабування	Зміна яскравості	Стиснення
Відсоток відновлених повідомлень	98%	95%	97%

Як бачимо з даної таблиці, відновлення повідомлень виконано у більшості випадків.

Висновок

Стеганографія – один з найперспективніших сучасних напрямів захисту інформації, наука, яка розвивається дуже швидко. Одним з основних критеріїв оцінки надійності стеганографічного методу є його стійкість до різноманітних видів атак. Останнім часом виділився такий напрям стеганографії як хеш-стеганографія, який базується на обчислювані хеш-коду цифрових зображень та повідомлення, що передається, та подальшому використанні отриманих хеш-кодів для передачі секретного повідомлення.

В роботі виконано модифікацію алгоритму хеш-стеганографії. Модифікований алгоритм засновано на використанні перцептивного хеш-алгоритму Simple Hash замість використання криптографічних хеш-функцій. Проведено аналіз ефективності модифікованого алгоритму, який показав, що модифікація забезпечує стійкість стеганоповідомлення до різних атак на відміну від оригіналу.

Список літератури

1. Carlo Blundo, Clemente Galdi - Theoretical Computer Science, Exploring New Frontiers of Theoretical Informatics, International Conference IFIP TCS 2000 – Pp.140-151.
2. Shin N. One-Time Hash Steganography / N. Shin // Springer-Verlag Berlin Heidelberg. – 2000 – Pp.17-28.
3. Testing Different Image Hash Functions [Електронний ресурс] // Режим доступу: https://content-blockchain.org/research/testing-different-image-hash-functions/.
4. Jie, Z. A Novel Block-DCT and PCA Based Image Perceptual Hashing Algorithm / Z. Jie // IJCSI International Journal of Computer Science Issues. – 2013. – V.10. – Pp. 399-403.
5. Standaert, F.X. Practical evaluation of a radial soft hash algorithm / F.X. Standaert, F. Lefebvre, G. Rouvroy, B.M. Macq, J.J. Quisquater, J.D. Legat // In Proceedings of the International Symposium on Information Technology: Coding and Computing (ITCC). – 2005. – V.2. – Pp. 89-94.
6. Marrand, D. Theory of edge detection / D. Marrand, E. Hildret // Proc. R. Soc. Lond. – 1980. – V.207. – Pp. 187-215.
7. Re-Hashed: The Difference Between SHA-1, SHA-2 and SHA-256 Hash Algorithms Read more at [Електроний ресурс] // Режим доступу : https://www.thesslstore.com/blog/difference-sha-1-sha-2-sha-256-hash-algorithms/.

МОДИФИКАЦИЯ АЛГОРИТМА ХЕШ-СТЕГАНОГРАФИИ

В.В. Зорило, М.В. Бохонько, А.И. Казаков

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: mishabahus28@gmail.com

Информация, которая передается по каналам связи, подвергается разнообразным угрозам, таким, как разоблачение, искажение и уничтожение. Одним из возможных решений проблемы угрозы разоблачения является использование стеганографических методов, которые в свою, очередь имеют свои ограничения по области применения. Стеганография предусматривает встраивание секретного сообщения в стеганографический контейнер (например, цифровое изображение) так, чтобы не нарушать устойчивость визуального восприятия контейнера. Одним из основных условий стеганографического метода является его устойчивость к различным видам атак. Современное направление стеганографии, хэш-стеганография, базируется на вычислении хэш-кода цифровых изображений и передаваемого сообщения, и дальнейшем использовании полученных хэш-кодов для шифрования секретного сообщения. Обычно большинство атак на цифровые изображения составляют опасность преимущественно для высоких частот, в

результате чего хэш-код цифрового изображения также будет претерпевать изменения, что может привести к частичной или полной потере стеганографического сообщения. Большинство современных методов получения хэш-кода цифрового изображения основаны на использовании высоких частот, что делает методы хэш-стеганографии уязвимыми к атакам по сравнению с оригиналом. Целью работы является повышение эффективности алгоритма хеш-стеганографии путем его модификации с помощью перцептивных хэш-алгоритмов. Проведен анализ существующих перцептивных хэш-алгоритмов для вычисления хэш-кода изображения. Выполнена модификация алгоритма хеш-стеганографии. Модифицированный алгоритм основан на использовании перцептивного хэш-алгоритма Simple Hash. Проведен анализ эффективности модифицированного алгоритма, который показал, что модификация обеспечивает повышение устойчивости стеганосообщения к различным атакам.
Ключевые слова: стеганография, хэш-стеганография, перцептивный хэш-алгоритм, встраивание дополнительной информации.

MODIFICATION OF THE HESH-STEGANOGRAPHY ALGORITHM

V.V. Zorilo, M.V. Bokhonko, A.I. Kazakov

Odessa National Polytechnic University,
Shevchenko Avenue, 1, Odessa, 65044, Ukraine; e-mail: mishabahus28@gmail.com

Abstract. Information transmitted through communication channels is subject to a variety of threats, such as exposure, distortion and destruction. One possible solution to the threat of autopsy is to use steganographic techniques, which in turn have limitations in scope. Steganography involves embedding a secret message in a steganographic container (for example, a digital image) so as not to violate the stability of the visual perception of the container. One of the main conditions of the steganographic method is its resistance to various types of attacks. The modern direction of steganography, hash steganography, is based on the calculation of the hash code of digital images and the transmitted message, and the further use of the received hash codes to encrypt the secret message. Typically, most digital image attacks are a high-frequency threat, causing the digital image hash code to be modified, which may result in partial or complete loss of the steganographic message. Most current digital imaging hash codes are based on high frequencies, making hash steganography vulnerable to attack. The purpose of this work is to increase the efficiency of the hash steganography algorithm by modifying it using perceptual hash algorithms. The analysis of existing perceptual hash algorithms for calculating the hash code of the image is performed. The hash algorithm has been modified. The modified algorithm is based on the use of the perceptual hash algorithm Simple Hash. The analysis of the effectiveness of the modified algorithm is carried out, which showed that the modification provides increased stability of the steganostation to various attacks.
Keywords: steganography, hash-steganography, perceptual hash algorithm, embedding additional information.