ISSN 2707-1898 (print)

Український журнал інформаційних технологій
Ukrainian Journal of Information Technology
http://science.lpnu.ua/uk/ujit
https://doi.org/10.23939/ujit2021.02.066
Article received 28.09.2021 p.
Article accepted 23.11.2021 p.
UDK 004:651.93

Correspondence author
I. M. Zhuravel
izhuravel@ukr.net

І. М. Журавель, Л. З. Мичуда, Ю. І. Журавель

Національний університет "Львівська політехніка", м. Львів, Україна

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СТЕГАНОГРАФІЧНОГО МЕТОДУ ПРИХОВУВАННЯ ДАНИХ ІЗ ЗАСТОСУВАННЯМ ІТЕРАЦІЙНИХ ФУНКЦІЙ ТА ДОДАВАННЯМ ШУМУ

Розвиток комп'ютерної та цифрової техніки сприяє зростанню інформаційних потоків, які передаються по відкритих та закритих каналах зв'язку. Здебільшого ця інформація має конфіденційний, фінансовий чи комерційний характер та представляє цінність для її власників. Це потребує розроблення механізмів захисту інформації від несанкціонованого доступу. Відомо два фундаментальні напрями безпечної передачі даних по відкритих каналах зв'язку – криптографія та стеганографія. Принципова різниця між ними полягає в цьому, що криптографія приховує від сторонніх зміст повідомлення, а стеганографія приховує сам факт передачі повідомлення. Розглянуто стеганографічні методи приховування даних, які є менш дослідженими, ніж криптографічні, проте володіють значним потенціалом щодо застосування у різноманітних прикладних задачах. Однією з важливих характеристик більшості методів є їх ефективність. Загалом ефективність оцінюють у контексті розв'язування конкретних задач. Проте найпоширенішими критеріями ефективності стеганографічних методів є обсяг приховуваних даних та спосіб передачі секретного ключа на приймальну сторону, який не дасть змоги зловмиснику його перехопити. Оскільки файли мультимедіа становлять значну частку об'єму трафіка мережі, то за стегоконтейнер вибрано цифрове зображення. Координати місця вбудовування запропоновано визначати на основі ітераційних функцій. Перевагою їх застосування є компактність опису координат пікселів, у які будуть приховуватися дані. Окрім цього, запропоновано застосувати алгоритм Діффі-Геллмана для передачі параметрів ітераційних функцій на приймальну сторону. Такий спосіб розподілу ключів робить стеганографічний метод менш вразливим до їх викрадення зловмисником. За другий критерій ефективності вибрано об'єм приховуваних даних. Встановлено, що помірне додавання мультиплікативного шуму дає можливість збільшити об'єм приховуваних даних без істотного зниження візуальної якості стегоконтейнера. Для аналізу спотворень на зображенні-стегоконтейнері, які обумовлені впливом шуму та модифікацією молодших розрядів пікселів, застосовано метод кількісної оцінки візуальної якості, який ґрунтується на законах зорового сприйняття.

Ключові слова: стеганографічне приховування даних; ефективність приховування; ітераційні функції; алгоритм Діффі-Гелмана.

Вступ

Одним із фундаментальних питань у процесі інформаційного забезпечення є захищена передача інформаційних потоків по каналах зв'язку, зокрема відкритих. Це питання обумовлено небажаною можливістю несанкціонованого доступу до каналів зв'язку та інформації, яка по них передається. Серед практичних задач цього напряму варто виділити непомітну передачу та приховане збереження інформації у цифрових носіях; формування індивідуальних відбитків у системах електронного документообігу з інформацією про те – хто, коли і які зміни вносив; нанесення водяних знаків у DLP-системах виявлення та запобігання витоку інформації; прихована передача прихованого сигналу у шкідливому програмному забезпеченні тощо.

Шифрування інформації не завжди може повною мірою вирішити описані вище задачі, оскільки не приховує самого факту їх передачі. У деяких випадках доцільніше застосовувати стеганографічні методи приховування та передачі інформації. Розвиток комп'ютерної та цифрової техніки призвели до того, що інтернет-мережі переповнені різноманітними цифровими медіафайлами – зображеннями, аудіо та відео, тому на сьогодні немає проблеми у виборі потенційного стеганоконтейнера. Однак розвиток інформаційних технологій призвів до появи нових методів стегоаналізу, які виявляють приховану стеганографічними методами інформацію. Тому *актуальним* є завдання підвищення ефективності стеганографічних методів, які б забезпечили вищий рівень приховуваності даних.

Об'єкт дослідження – стеганографічне приховування даних у цифрових зображеннях.

Предмет дослідження – методи, моделі, алгоритми підвищення ефективності вбудовування інформації у графічні стегоконтейнери.

Мета роботи – підвищення ефективності стеганографічного приховування інформації через застосування ітераційних функцій під час формування координат місць вбудовування та додаванні шуму зображення. Це дасть змогу синтезувати таку модель стеганографічного приховування даних, де інформація про координати їх вбудовування, які становить секретний ключ, займатиме значно менший обсяг, що приводитиме до мінімізації можливості перехоплення її зловмисником. Додавання шуму на зображення надасть змогу збільшити об'єм вбудованих даних без істотного зниження візуальної якості стеганоконтейнера.

Для досягнення зазначеної мети визначено такі *основні завдання дослідження*:

- розробити моделі підвищення ефективності методу стеганографічного приховування інформації з використанням системи ітераційних функцій та додаванням шуму на зображення;

- адаптувати метод кількісного оцінювання візуальної якості до аналізу заповненого стеганоконтейнера спотвореного шумом;
- встановити залежність візуальної якості зображень-контейнерів від рівня вбудованого мультиплікативного шуму та об'єму вбудованих даних, яка і визначатиме ефективність стеганографічного методу.

Наукова новизна отриманих результатів дослідження – розроблено метод стеганографічного вбудовування даних у цифрове зображення, який через застосування ітераційних функцій і накладання мультиплікативного шуму забезпечує вищу приховуваність секретного ключа та надає можливість збільшити об'єм вбудовуваної інформації, що загалом призводить до підвищення ефективності стегоалгоритму.

Практична значущість результатів дослідження – застосування ітераційних функцій та алгоритму Діффі-Геллмана у стегоалгоритмі унеможливить перехоплення секретних ключів зловмисником, а застосування шуму дасть змогу збільшити об'єм вбудовуваних даних у зображення-стегоконтейнер.

Матеріали та методи дослідження. Основні *методи досліджень*, які застосовуються у роботі, – оброблення та аналіз цифрових зображень і теорія фракталів.

Аналіз останніх досліджень та публікацій. Розвиток цифрової техніки та комп'ютерних технологій стимулює проведення досліджень задач зі стеганографії. Переважна більшість робіт спрямована на підвищення ефективності методів стеганографічного приховування даних через відповідне подання контейнеру [5], [7], застосування генетичних алгоритмів для оптимізації об'ємів вбудованої інформації [8], використання стеганографічних методів приховування у різних прикладних галузях [4] тощо. Останніми роками активно проводяться дослідження у напрямі мережевої стеганографії [1], де важливим є вибір об'єкту для вбудовування з врахуванням особливостей протоколу передачі даних по мережі. Приховування інформації реалізовується у різних цифрових носіях, зокрема в аудіофайлах. Аудіостеганографія є одним із перспективних напрямів приховування даних [6]. Важливою особливістю під час побудови стеганосистеми є дотримання компромісу між непомітністю вбудовування та низькою обчислювальною складністю [3]. Зважаючи на поширеність відеофайлів, актуальною, особливо з погляду приховування великих об'ємів даних, є відеостеганографія [9].

Здійснений аналіз виявив, що недостатньо уваги в наукових дослідженнях приділено одному з найбільш фундаментальних питань стеганоганографії – вибору місць вбудовування інформації, координати яких виступають як секретний ключ та спосіб його передачі на приймальну сторону. Також недостатньо опрацьованими є дослідження щодо збільшення об'ємів приховуваної інформації.

Результати дослідження та їх обговорення

Як зазначалося вище, здешевлення цифрової техніки призводять до лавиноподібного зростання кількості інформаційних потоків, які передаються по мережах. Для інформаційного убезпечення даних, що передаються по комп'ютерних мережах, застосовують криптографію та стеганографію. В обох випадках фундаментальним є питання формування секретних ключів та передачі їх від передавальної до приймальної сторін. У методі стеганографічного приховування даних у цифрових зображеннях секретним ключем є набір координат пікселів, які будуть модифіковані через вбудовування даних. Це справедливо для випадку вбудовування даних у просторовій області, для випадку вбудовування у частотній області – підхід буде аналогічним. Якщо секретні ключі будуть перехоплені зловмисником, то скомпрометованим буде і приховане повідомлення.

Сформуємо вимоги до синтезу і передачі секретних ключів. У випадку вбудовування зображення у зображення методом модифікації найменш значущих біт, об'єм імплементованих даних здебільшого є доволі значним. Це призводить до того, що кількість координат пікселів, куди ця інформація буде вбудовуватися і які виступають як секретні ключі, є також достатньо великою, що збільшує імовірність їх перехоплення. Отже, актуальною є задача зменшення об'єму інформації про секретні ключі без зменшення їхньої кількості. Для цього у роботі запропонували застосувати математичний апарат теорії фракталів, а саме систему ітераційних функцій [2]. Загалом одну з найбільш простих ітераційних функцій можна представити так:

$$\begin{aligned} X' &= A \cdot X + B \cdot Y + C \\ Y' &= D \cdot X + E \cdot Y + F \end{aligned}. \qquad (1)$$

Вираз (1) представляє собою афінні перетворення площини. Також вираз (1) відображає перетворення однієї багатовимірної множини в іншу. Системи ітераційних функцій мають багато інших застосувань, зокрема вони лежать в основі методів фрактального стиску зображень. Для випадку стеганографічного приховування, систему ітераційних функцій використаємо для формування координат (x, y) пікселів зображення, у які буде вбудовуватися інформація. Замість об'ємної множини координат, яка представляє собою секретний ключ, на приймальну сторону буде передаватися система ітераційних функцій у вигляді її параметрів. Для найпростіших ітераційних функцій ці параметри складаються зі шести значень – *A, B, C, D, E, F*. Кількість ітерацій функції (1) визначається об'ємом даних, які необхідно приховати у зображенні-стегоконтейнері.

Отже, застосування ітераційних функцій (1) дає можливість у рази зменшити кількість інформації про координати приховування даних, зменшуючи таким чином її вразливість до несанкціонованого доступу.

Недоліком представленої вище моделі формування координат пікселів для вбудовування даних є те, що у випадку, коли зловмисник дізнається параметри *A, B, C, D, E, F* ітераційної функції (1), то йому стануть відомі координати пікселів з прихованою інформацією.

Для усунення цього недоліку параметри *A, B, C, D, E, F* з ітераційної функції (1), які у розроблюваному стеганографічному методі інтерпретуються як секретні ключі, пропонуємо формувати згідно з протоколом Діффі-Геллмана. Це дасть змогу згенерувати параметри *A, B, C, D, E, F* на передавальній та приймальній сторонах, використовуючи не захищені від прослуховування канали зв'язку.

Модель підвищення ефективності методу стеганографічного приховування інформації з використанням системи ітераційних функцій. На основі представленого вище опису синтезу і передачі секретних ключів сформували функціональну модель методу стеганогра-

фічного приховування інформації, яку навели на рис. 1. Загалом вона складається з трьох основних кроків.

На першому кроці передавальна та приймальна сторони, згідно з відомим протоколом Діффі-Геллмана, формують параметри *A, B, C, D, E, F*, які застосовуються у системі ітераційних функцій (1). На другому кроці генерується набір координат пікселів, у які буде приховуватися інформація. Серед головних переваг такого способу генерації варто виділити те, що інформація про координати місць вбудовування не передається по мережі, а отже, не може бути перехоплена зловмисником.

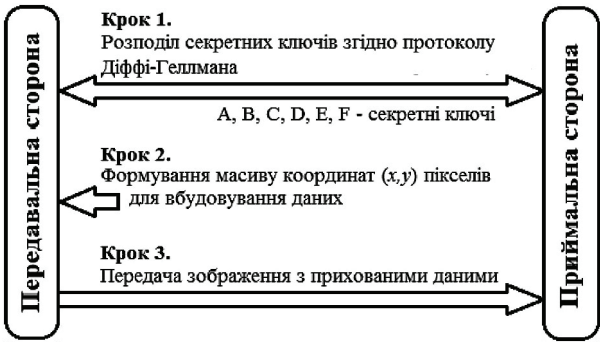

Рис. 1. Функціональна модель пропонованого методу стеганографічного приховування інформації

Як вже зазначали вище, у цій роботі застосовуємо метод приховування даних у найменш значущий біт пікселів цифрового зображення. Перші два кроки накладають свої особливості на реалізацію третього кроку. Їхня суть полягає у відмінностях підходів до вибору місць вбудовування приховуваних даних. У більшості відомих стеганографічних методів дані приховуються у високочастотні ділянки зображення. З одного боку, такий підхід забезпечує більш ефективну приховуваність даних через візуальну непомітність спотворень стеганоконтейнера. З іншого боку, високочастотні ділянки достатньо легко локалізувати на зображенні, а їх подальше опрацювання низькочастотним фільтром призводить до повної втрати вбудованої інформації. Згідно із запропонованим у роботі підходом координати пікселів, у які буде вбудовуватися інформація, розміщені по всьому полю зображення і визначаються тільки параметрами *A, B, C, D, E, F*, значення яких, згідно з алгоритмом Діффі-Геллмана, не передаються по мережі, а отже, не можуть бути відомі зловмиснику.

Підвищення ефективності стеганографічного приховування даних також можливо досягнути через додавання шуму на зображення-стеганоконтейнер. Це збільшить частку високочастотних складових на зображенні та дасть змогу вбудовувати більші об'єми даних. Водночас, зростання шумової складової на зображенні призведе до зниження візуальної якості стеганоконтейнера. Це потребує провести дослідження, що дадуть відповідь на питання – який шум та якого рівня додавати на зображення-стеганоконтейнер, щоб мати змогу збільшити кількість вбудовуваної інформації, але не вносити істотні візуальні спотворення.

Модель підвищення ефективності методу стеганографічного приховування інформації з додаванням шуму на зображення. Спочатку необхідно вибрати зображення-стеганоконтейнер, куди буде приховуватися інформація. У цій роботі застосували стеганографічний метод приховування у найменш значущі біти. Оскільки вбудовування будемо здійснювати в просторовій області, то ця обставина обумовить додаткові вимоги до вибору стеганоконтейнера. Зображення-стеганоконтейнер має містити високочастотні ділянки. Чим більше таких ділянок буде на зображенні, тим більш ефективним буде приховування даних стосовно візуального сприйняття. Загалом кількість пікселів у високочастотних ділянках зображення має бути достатньою для приховування потрібного об'єму даних. Цю вимогу щодо зображення можна формалізувати, але на практиці здебільшого вибір стеганоконтейнера здійснює дослідник, ґрунтуючись на своїх знаннях та вміннях. З урахуванням висунутих вище вимог у роботі вибрали зображення-стеганоконтейнер, яке представили на рис. 2 і охарактеризували наявністю великої кількості дрібних деталей.

Рис. 2. Зображення-стеганоконтейнер

Як зазначали вище, головною ознакою стеганографії є прихована передача інформації. Надійність приховування визначатиме ефективність стеганографічної системи. Сама ж надійність приховування залежить від багатьох факторів – місця вбудовування, вибору стеганоконтейнера, розміру вбудовуваного повідомлення тощо.

Для підвищення ефективності приховування даних, згідно з висунутою вище гіпотезою, додамо на зображення-стегоконтейнер шум. Сформуємо дві серії зображень – у першій серії додамо на зображення різні рівні шуму типу "сіль та перець", а у другій серії – різні рівні мультиплікативного шуму (рис. 3).

Візуальний аналіз зображень з накладеним шумом показує, що шум типу "сіль та перець" вносить на зображення помітніші спотворення. Причому ці спотворення стають помітними навіть за невеликого відсотка спотворених пікселів. Мультиплікативний шум є менш помітним на зображенні, порівняно з імпульсним.

Для числової оцінки внесених у зображення спотворень використовуємо середньоквадратичне відхилення

$$RMS = \sqrt{\frac{1}{3 \cdot n \cdot l} \sum_{k=1}^{3} \sum_{i=1,\, j=1}^{n,l} \left(x_{ijk} - y_{ijk} \right)^2} \qquad (2)$$

та співвідношення сигнал/шум

$$PSNR = 10 \log_{10} \frac{3 \cdot (2^B - 1)^2 \cdot n \cdot l}{\sum_{k=1}^{3} \sum_{i=1,\, j=1}^{n,l} \left(x_{ij} - y_{ij} \right)^2}, \qquad (3)$$

де i та j – координати пікселя, а k – номер колірного шару зображення.

Результати проведених обчислень, згідно з виразами (1) та (2), навели на рис. 4. З поданих на цьому рисунку графіків видно, що різні типи шумів вносять різний рівень візуальних спотворень на зображеннях. Кількісні значення середньоквадратичних відхилень RMS, які обчислені для зображень з імпульсними та мультиплікативними шумами, відрізняються, а їхні графіки мають різний характер у разі збільшення рівня шумів.

Рис. 3. Серії зображень з накладеним шумом типу: "сіль та перець" (1-5) та відповідною часткою спотворених пікселів *n*; мультиплікативним шумом (6-10) та відповідною дисперсією D

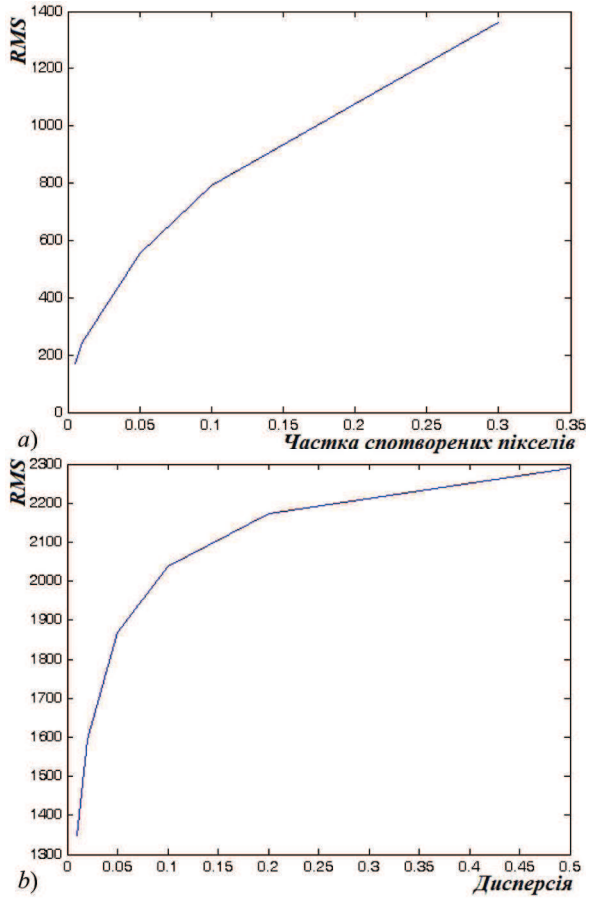

Рис. 4. Кількісне оцінювання спотворень на зображеннях (рис. 3), які внесені різними рівнями імпульсного (*a*) та мультиплікативного (*b*) шумів.

Отримані результати виявили таку суперечність. Порівняємо два зображення – на рис. 3.*5* та на рис. 3.4. Для зображення з мультиплікативним шумом (рис. 3.4) рівень середньоквадратичного відхилення *RMS* становить 2171,5, а для зображення з накладеним імпульсним шумом (рис. 3.*5*) *RMS* = 1360, тобто в 1,6 раза менше. Проте, візуальний аналіз показує зворотне, що зображення з накладеним імпульсним шумом (рис. 3.*5*) містить більше спотворених об'єктів та має нижчу візуальну якість порівняно із зображенням, на яке був накладений мультиплікативний шум (рис. 3.4).

Отже, наведені вище вирази (2) та (3) є зручними у використанні, але вони не враховують закони візуального сприйняття, тому не можуть бути об'єктивною мірою візуальних спотворень модифікованих контейнерів. Також недоліком використання *RMS* для оцінювання спотворень на зображенні є те, що ця оцінка є не чутливою до локальних змін на зображенні. Отже, доцільним є застосування такої кількісної оцінки спотворень, яка б враховувала особливості візуального сприйняття зображень людиною. Для цього у роботі запропонували використовувати метод кількісного оцінювання якості візуального сприйняття зображення [11]

$$Q_p = \frac{1}{|1+a|}\cdot\left(1-\frac{1}{1+b}\right)\cdot\frac{1}{1+c}\cdot\frac{1}{1+d}, \qquad (4)$$

де $a = M[(L-R/2)]$; $b = M[(L-R/2)^2]$;

$$c = \frac{M[(L-R/2)^3]}{(\sqrt{M[(L-R/2)^2]})^3}; \quad d = \frac{M[(L-R/2)^4]}{(\sqrt{M[(L-R/2)^2]})^4} - 3;$$

$$M[(L-A)^s] = \frac{1}{LMAX^s}\sum_{L=0}^{LMAX}(L-A)^s H(L)\cdot$$

У наведених вище виразах L – інтенсивність елемента зображення; $H(L)$ – розподіл інтенсивностей елементів зображення; s – порядок моментів; A – величина, щодо якої визначається момент.

Застосуємо вираз (4) для оцінювання візуальної якості зображень-стеганоконтейнерів (рис. 3), які спотворені імпульсним та мультиплікативним шумами. Результати обчислень наведено в таблиці.

Таблиця. Результати оцінювання візуальної якості зображень-стеганоконтейнерів, які були спотворені імпульсним та мультиплікативним шумами

Зображення з накладеним імпульсним шумом	Кількісна оцінка візуальної якості, *Q*	Зображення з накладеним мультиплікативним шумом	Кількісна оцінка візуальної якості, Q
Рис. 3.1	2,0009	Рис. 3.6	1,9854
Рис. 3.2	2,0071	Рис. 3.7	1,9891
Рис. 3.3	2,0544	Рис. 3.8	1,9992
Рис. 3.4	2,1010	Рис. 3.9	2,0062
Рис. 3.5	2,2498	Рис. 3.4	2,0092

Для наочності відобразимо результати, які наведено у таблиці, у вигляді графіка (рис. 5).

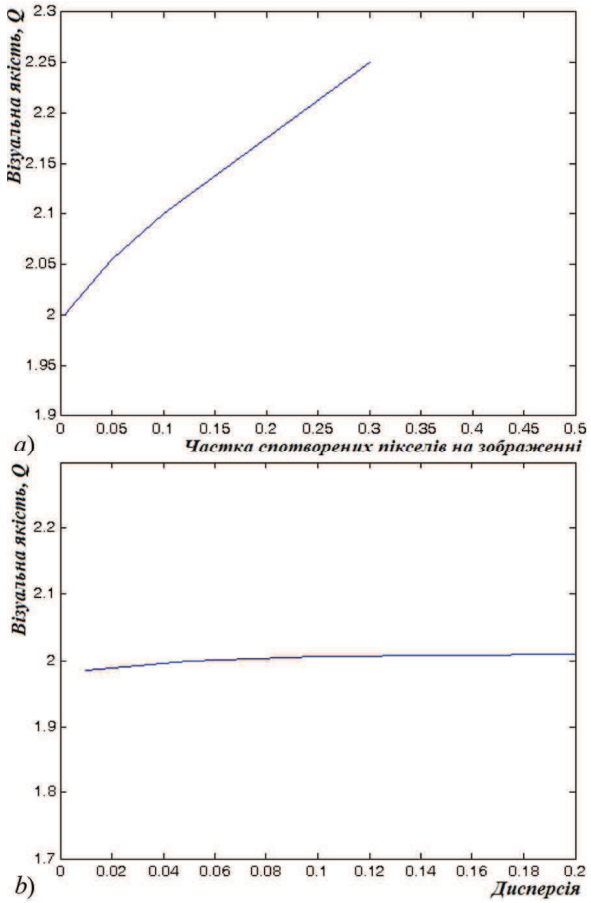

Рис. 5. Результати кількісного оцінювання візуальної якості порожніх зображень-контейнерів, які спотворені імпульсними (*a*) та мультиплікативними (*b*) шумами із застосуванням виразу 4

Проаналізуємо отримані на рис. 5 результати. Як бачимо з рис. 5,*a* кількісні оцінки зображень-контейнерів (рис. 3) зростають у разі збільшення рівня імпульсного шуму, що не відповідає та суперечить їх візуальній оцінці.

Отже, ні відомий та широковживаний вираз середньоквадратичного відхилення *RMS* (2), ні вираз кількісного оцінювання якості на основі моментів (4) не забезпечують коректних результатів обчислень та не можуть застосовуватися для оцінювання візуальної якості зображень-контейнерів, які спотворені імпульсним та мультиплікативним шумами. Причина полягає у тому, що в основі цих методів використовуються різницеві вирази інтенсивностей, які збільшення шумових викидів сприймають як підвищення контрастності, а відповідно, і зростання візуальної якості зображень.

Це призводить до потреби модифікації описаного вище методу кількісного оцінювання якості на основі моментів для оцінювання зашумлених зображень

$$Q' = 4 - Q. \qquad (5)$$

На рис. 6 навели результати кількісного оцінювання візуальної якості зашумлених зображень-контейнерів із застосуванням виразу (5).

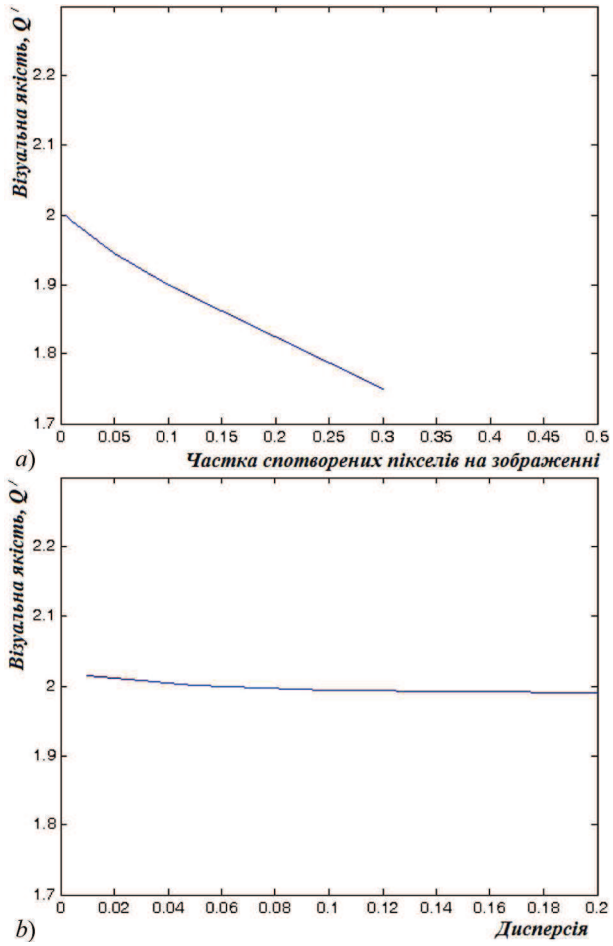

Рис. 6. Результати кількісного оцінювання візуальної якості порожніх зображень-контейнерів, які спотворені імпульсними (*a*) та мультиплікативними (*b*) шумами із застосуванням виразу (5)

Наведені на рис. 6 результати кількісного оцінювання візуальної якості порожніх зображень-контейнерів, які спотворені імпульсними (*a*) та мультиплікативними (*b*) шумами із застосуванням виразу (5), добре корелюють із візуальною оцінкою, а саме – зростання рівня зашумленості призводить до зниження візуальної якості. Причому зниження візуальної якості є більш помітним у разі зростання кількості пікселів, які спотворені імпульсним шумом. Отже, надалі будемо застосовувати запропонований вираз (5) для кількісного оцінювання візуальної якості зашумлених стеганоконтейнерів. Дослідимо гіпотезу, згідно з якою додавання мультиплікативного шуму на зображення не знижує істотно візуальну якість, але мало б дозволити збільшення об'єму вбудованих даних.

Комп'ютерне моделювання розробленого методу та обговорення результатів дослідження. Провели комп'ютерне моделювання методу стеганографічного приховування даних з урахуванням описаних вище у роботі способів підвищення їх ефективності.

За стегоконтейнер вибрали зображення, яке навели на рис. 2. У це зображення вбудовувалося коротке текстове повідомлення. Приховування здійснювалося у високочастотні ділянки зображення (рис. 7,*a*) та у пікселі, координати яких визначали із застосуванням ітераційних функцій (1) (рис. 7,*b*).

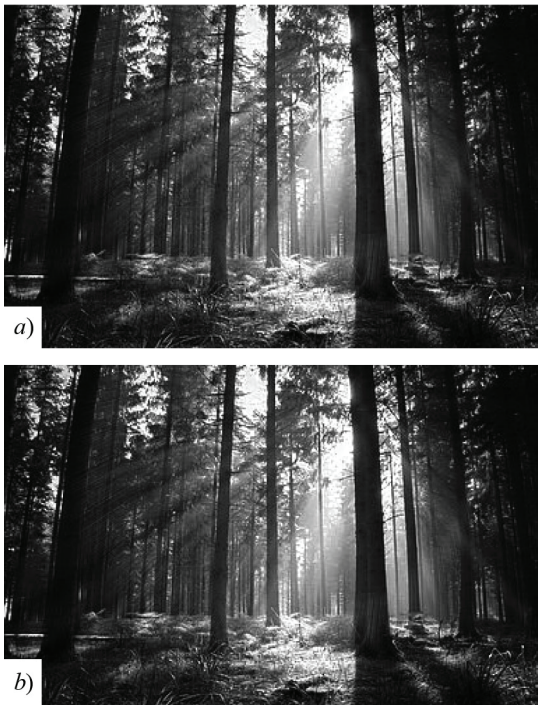

Рис. 7. Приховування інформації у високочастотні ділянки зображення (*a*) та у пікселі, координати яких визначали із застосуванням ітераційних функцій (1) (*b*)

Зображення з вбудованими даними на рис. 7,*а* та 7,*б* візуально практично не відрізняються від порожнього стегоконтейнера (рис. 2). Це відповідає фундаментальному завданню стеганографії, яке полягає у непомітному візуальному приховуванні даних. Оскільки стеганоконтейнер містить достатньо багато високочастотних ділянок, то спосіб вибору місця вбудовування не впливає на якість візуального приховування невеликих обсягів інформації. Проте стосовно передачі секретних ключів із передавальної на приймальну сторін, очевидну перевагу має модель з використанням системи ітераційних функцій та протоколу Діффі-Геллмана.

У роботі також дослідили вплив об'єму вбудованого повідомлення на ефективність методу стеганографічного приховування даних, а саме візуальну якість заповненого контейнера.

Виконаємо такі експерименти – спочатку повідомлення різного об'єму вбудуємо у вхідне незашумлене зображення-стеганоконтейнер (рис. 2). Далі будемо накладати шум на стеганоконтейнер, збільшувати його рівень та вбудовувати повідомлення різних об'ємів.

Під час таких досліджень необхідно враховувати співвідношення об'єму зображення – контейнера та об'єму вбудовуваного повідомлення.

Вхідне зображення-стеганоконтейнер (рис. 2) займає 91 кілобайт. Вбудовані дані у вигляді текстового повідомлення займають відповідно 1 %, 5 %, 10 %, 20 % та 40 % від об'єму зображення-стеганоконтейнера. На вхідне зображення додаємо мультиплікативний шум з різним рівнем дисперсії – від 0,05 до 0,1. Вибір мультиплікативного шуму обумовлений тим, що збільшення частки цього типу шуму не так сильно зменшує візуальну якість, як інші типи шумів, зокрема імпульсний. Це ми довели вище у цій роботі експериментально.

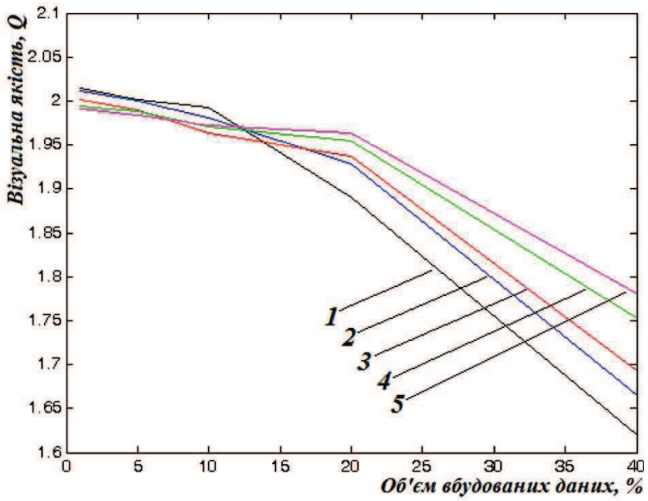

Рис. 8. Графіки залежності візуальної якості зображень-контейнерів від рівня вбудованого мультиплікативного шуму (1-5) та об'єму вбудованих даних

Обговорення результатів дослідження. Проаналізуємо отримані на рис. 8 результати обчислення візуальної якості зображень-контейнерів за різних рівнів вбудованого мультиплітативного шуму та об'єму вбудованих даних.

Як зазначали вище, на порожні зображення-стеганоконтейнери накладали різні рівні мультиплікативного шуму (рис. 3). Збільшення рівня шуму погіршує якість зображення, але не так інтенсивно, як для випадку імпульсного шуму. Після вбудовування даних у стеганоконтейнери з різним рівнем зашумленості було виявлено такі закономірності – чим більш зашумленим був порожній стеганоконтейнер, тим повільніше спадає рівень візуальної якості внаслідок збільшення об'єму вбудованих даних. Отже, накладення мультиплікативного шуму з невеликою дисперсією призводить до можливості приховування більших (до 12 %) об'ємів інформації без зниження візуальної якості стегозображення. Результати порівняння отримали на основі аналізу запропонованого у роботі та відомого методу приховування інформації у найменш значущий біт [10]. Варто зауважити, що оцінка візуальної якості зображення-контейнера залежатиме також від їх семантичного наповнення. Проте всі виявлені тенденції зміни оцінки візуальної якості, залежно від накладеного шуму та об'єму вбудованого повідомлення, будуть збережені.

Висновок

На основі виконаних у роботі досліджень розроблено моделі підвищення ефективності методу стеганографічного приховування інформації з використанням системи ітераційних функцій та додаванням шуму на зображення-стеганоконтейнер. За допомогою ітераційних функцій визначають координати пікселів для приховування даних. Перевагою застосування ітераційних функцій є це, що їх описують невеликою кількістю параметрів, які передаються на приймальну сторону за допомогою алгоритму Діффі-Геллмана. Це приводить до цього, що секретні ключі не передаються по каналу зв'язку, а отже, не можуть бути перехопленими зловмисником. Також у роботі встановлено, що незначне додавання мультиплікативного шуму дає можливість збільшити об'єм приховуваних даних без істотного зниження візуальної якості стегоконтейнера. Для аналізу спотворень стегоконтейнера застосовано метод кількісного оцінювання візуальної якості цифрових зображень, який був адаптований для дослідження зашумлених даних.

References

[1] Frączek, Wojciech, & Szczypiorski, Krzysztof (2016). Perfect undetectability of network steganography. Security Comm. Networks, 9: 2998-3010. https://doi.org/10.1002/sec.1491

[2] Grinchenko, V. T., Matcypura, V. T., & Snarskii, A. A. (2013). Fraktaly: ot udivleniia k rabochemu instrumentu. Naukova dumka, Kyiv, 270 p. [In Russian].

[3] Kadhimab, I. J., Premaratne, P., James, P., & Halloran, Vial & B. (2019). Comprehensive Survey of Image Steganography: Techniques, Evaluations, and Trends in Future Research. *Neurocomputing, 335*, 299–326. https://doi.org/10.1016/j.neucom.2018.06.075

[4] Manju, Khari, Aditya, Kumar, Garg, Amir, Gandomi, H., Gupta, Rashmi, Patan, Rizwan, & Balusamy, Balamurugan (2020). Securing Data in Internet of Things (IoT) Using Cryptography and Steganography Techniques. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 50*(1), 73–80. https://doi.org/10.1109/TSMC.2019.2903785

[5] Saravanan, M., & Priya, A. (2019). An Algorithm for Security Enhancement in Image Transmission Using Steganography. *Journal of the Institute of Electronics and Computer, 1*, 1–8. https://doi.org/10.33969/JIEC.2019.11001

[6] Sedighi Vahid, Cogranne Rémi, Fridrich Jessica (2016). Content-Adaptive Steganography by Minimizing Statistical Detectability. *IEEE Transactions on Information Forensics and Security, 11*(2), 221–234. https://doi.org/10.1109/TIFS.2015.2486744

[7] Sonal, G., & Mer, H. (2017). A survey: Image Steganography using different method. *International Journal of Novel Research and Development, 2*(4), 48–51.

[8] Wazirali, A., Alasmary, W., Mahmoud, M. E. A., & Alhindi, A. (2019). An Optimized Steganography Hiding Capacity and Imperceptibly Using Genetic Algorithms. *IEEE Access, Special Section on Security, Privacy, and Trust Management in Smart Cities, 7*, 1–13. https://doi.org/10.1109/ACCESS.2019.2941440

[9] Yunxia, L., Shuyang, L., Yonghao, W., Hongguo, Z., & Sia, L. (2019). Video steganography: A review. *Neurocomputing, 335*, 238–250. https://doi.org/10.1016/j.neucom.2018.09.091

[10] Zhou, Ri-Gui, Hu, Wenwen, & Fan, Ping (2017). Quantum watermarking scheme through Arnold scrambling and LSB steganography. *Quantum Information Processing, 16*, article number 212. https://doi.org/10.1007/s11128-017-1640-9

[11] Zhuravel, I. M., & Vorobel, R. A. (2001). Kilkisna otsinka yakosti zobrazhen. Pratsi IV Serednoievropeiskoi konferentsii "Kompiuterni metody i systemy v avtomatytsi i elektrotekhnitsi". CHastyna 1. CHenstokhova, Polsha, 17-18 veresnia, 2001. [In Ukrainian].

I. M. Zhuravel, L. Z. Mychuda, Yu. I. Zhuravel
Lviv Polytechnic National University, Lviv, Ukraine

IMPROVING THE EFFICIENCY OF THE STEGANOGRAPHIC METHOD OF DATA HIDING WITH THE APPLICATION OF ITERATIVE FUNCTIONS AND NOISE ADDITION

The development of computer and digital technology contributes to the growth of information flows transmitted through open and closed communication channels. In many cases, this information is confidential, financial, or commercial in nature and is of value to its owners. This requires the development of mechanisms to protect information from unauthorized access. There are two fundamental areas of secure data transmission over the open communication channels – cryptography and steganography. The fundamental difference between them is that cryptography hides from others the content of the message, and steganography hides the very fact of the message transmission. This paper is devoted to steganographic methods of data concealment, which are less researched than cryptographic, but have significant potential for use in a variety of applications. One of the important characteristics of most methods is their effectiveness. In general, efficiency is assessed in the context of solving specific problems. However, the most common criteria for the effectiveness of steganographic methods are the amount of hidden data and the method of transmitting the secret key to the receiving party, which will not allow the attacker to intercept it. Because media files make up a significant portion of network traffic, a digital image is chosen as the stegocontainer. It is proposed to determine the coordinates of the embedding location on the basis of iterative functions. The advantage of their use is the compactness of the description of the coordinates of the pixels in which the data will be hidden. In addition, it is proposed to use the Diffie-Gellman algorithm to transfer the parameters of iterative functions to the receiving side. This method of key distribution makes the steganographic method less vulnerable to being stolen by an attacker. The second performance criterion is the amount of hidden data. The paper found that the moderate addition of multiplicative noise makes it possible to increase the amount of hidden data without significantly reducing the visual quality of the stegocontainer. To analyze the distortions in the image-stegocontainer, which are due to the influence of noise and modification of the lower bits of pixels, the method of a quantitative assessment of visual quality is used, which is based on the laws of visual perception.

Keywords: steganographic data hiding; hiding efficiency; iterative functions; Diffie-Gelman algorithm.

Інформація про авторів:

Журавель Ігор Михайлович, д-р техн. наук, ст. наук. співробітник, професор, кафедра безпеки інформаційних технологій. **Email:** izhuravel @ukr.net; https://orcid.org/0000-0003-1114-0124

Мичуда Леся Зиновіївна, д-р техн. наук, доцент, професор, кафедра безпеки інформаційних технологій. **Email:** lesyamychuda@yahoo.com; https://orcid.org/0000-0001-8266-1782

Журавель Юрій Ігорович, студент, кафедра безпеки інформаційних технологій. **Email:** yura_zhur@ukr.net

Цитування за ДСТУ: Журавель І. М., Мичуда Л. З., Журавель Ю. І. Підвищення ефективності стеганографічного методу приховування даних із застосуванням ітераційних функцій та додаванням шуму. *Український журнал інформаційних технологій.* 2021, т. 3, № 2. С. 66–73.

Citation APA: Zhuravel, I. M., Mychuda, L. Z., & Zhuravel, Yu. I. (2021). Improving the efficiency of the steganographic method of data hiding with the application of iterative functions and noise addition. *Ukrainian Journal of Information Technology, 3*(2), 66–73. https://doi.org/10.23939/ujit2021.02.066