УДК 004.056 doi: 10.20998/2220-4784.2021.02.04

О. С. КРАВЧЕНКО

ЗАГАЛЬНА ТЕХНОЛОГІЯ ШИФРУВАННЯ ТА ВБУДОВУВАННЯ ДАНИХ В РАСТРОВІ ЗОБРАЖЕННЯ, ЩО Є СТІЙКИМ ДО СТИСНЕННЯ JPEG

Об’єктом дослідження представленої статті є стеганографічні методи організації прихованого каналу зв'язку в каналі загального користування, що забезпечують стійкість до стиснення з втратами. Мета роботи – розробка алгоритму вбудовування даних в растрові зображення, стійкого до JPEG стискання та атакам на контейнер. У роботі досліджено особливості роботи алгоритму JPEG, проаналізовано стеганографічні методи захисту інформації та побудовано стеганографічний алгоритм, стійкий до JPEG стискання та атакам на контейнер. Додаткову надійність забезпечують поліалфавітний шифр підстановки і користувацький секретний ключ, що використовуються для шифрування вихідного повідомлення. Алгоритм було розроблено за допомогою мови програмування Python 3, бібілотек NumPy, SciPy, MatPlotLib та пакету Jupyter Lab. Задачу було виконано за допомогою стандартних математичних та статистичних методів та засобів високорівневої мови програмування Python 3.

Ключові слова: стеганографія, крітографія, JPEG алгоритм, стійкість стеганографічного контейнера, вбудовування даних в растрові зображення, стегоаналіз.

Вступ.

Цифрові пристрої та Інтернет використовують у різновидах промислових підприємствах, приватної і державної форм власності з метою скорочення трудових ресурсів і підвищення ефективності роботи, а також для обміну інформацією. У зв'язку з цим є актуальним питання захисту цифрової інформації, що передається. Наприклад, відправник зашифровує інформацію на своєму боці і передає одержувачу, який розшифровує її за допомогою ключа, яким сторони попередньо обмінялися і також існують методи захищеного обміну ключами через відкритий канал зв'язку. Однак, у такого підходу є один істотний недолік – зашифровані дані виглядають як безладний набір символів, чим залучають потенційну увагу зацікавлених осіб, чиєю метою може стати їх розшифрування. Таким чином, технології шифрування не вирішують проблему захищеної передачі конфіденційної інформації повністю. Необхідний метод, що дозволяє передавати дані під виглядом інших даних і тим самим не привертає увагу до повідомлення – наука стеганографія. Методи стеганографії не тільки дозволяють приховано зберігати і передавати інформацію, але і дуже успішно допомагають вирішити питання захисту інформації від несанкціонованого копіювання, відстеження поширення інформації в мережі загального користування, пошуку даних в мультимедійних базах даних і т.д..[1]

Постановка проблеми у загальному вигляді та її зв’язок із важливими науковими та практичними завданнями. Метою даного дослідження є розробка алгоритму шифрування та вбудовування даних в растрові зображення, стійкого до JPEG стискання. Розвиток Інтернет-технологій і сучасна інформаційна ера визначили нові стандарти життя, тепер промислові та економічні, приватні і державні підприємства активно використовують Інтернет для обміну інформацією. У зв'язку з цим є актуальним питання захисту цифрової інформації, що передається. Існує різноманітність криптографічних методів для захищеного обміну інформацією, умовою яких є шифрування всіх даних, що проходять через канал зв'язку. Однак, у такого підходу є один істотний недолік – зашифровані дані виглядають як безладний набір символів, чим залучають потенційну увагу зацікавлених осіб, чиєю метою може стати їх розшифрування. Таким чином, технології шифрування не вирішують проблему захищеної передачі конфіденційної інформації повністю. Необхідний метод, що дозволяє передавати дані під виглядом інших даних і тим самим не привертає увагу до повідомлення, одночасно підтримуючи шифрування.

Стеганографування може здійснюватися різними способами, спільною рисою яких є те, що конфіденційна інформація вбудовується в деякий контейнер, що не привертає уваги. Результатом вбудовування є стеганоповідомлення, яке передається по каналу зв'язку або зберігається в отриманому вигляді.

У даній роботі в якості контейнера розглядаються растрові зображення, як один з найбільш популярних типів мультимедійних файлів, що передаються через Інтернет. Оскільки при передачі через сторонні сервіси зображення часто стискаються з втратами для зменшення трафіку, записана в них інформація може бути знищена. Таким чином, завдання створення алгоритму вбудовування даних в растрові зображення, який був би стійким до стиснення з втратами до певної межі, є актуальною.

Оскільки JPEG стиснення відноситься з стиснення з втратами, при якому певна інформація зображення втрачається, необхідно проаналізувати алгоритм його роботи і визначити, якими методами можна вбудувати інформацію в зображення таким чином, щоб вона не була повністю знищена при стисненні. Під аналізом мається на увазі детальне вивчення схеми роботи алгоритму і обчислення тих областей зображення, стиснення до яких застосовується з найменшими втратами.

© Кравченко О.С., 2021

Відповідно до технічного завдання встановлені наступні задачі (табл. 1). [2]

Таблиця 1 – Складові дослідження за темою проекту

№	ЗМІСТ
1	ПОСТАНОВКА ЗАДАЧІ
2	ТЕОРЕТИЧНІ ВІДОМОСТІ: Сучасні методи стеганографії і їх використання; Аналіз роботи алгоритму JPEG
3	РОЗРОБКА АЛГОРИТМУ: Аналіз частотних методів цифрового маркування; Проектування частотного стеганографічного алгоритму; Використання принципу математичного залишку для підвищення стійкості алгоритму
4	ПІДТРИМКА ШИФРУВАННЯ ВИХІДНИХ ДАНИХ: Огляд криптографічних методів шифрування; Використання поліалфавітного шифру підстановки
5	АНАЛІЗ ЕФЕКТИВНОСТІ І СТІЙКОСТІ РОЗРОБЛЕНОГО АЛГОРИТМА: Аналіз стійкості алгоритму до стискання JPEG; Аналіз стійкості алгоритму до дешифрування
6	ВИСНОВКИ

ПРИНЦИП РОБОТИ JPEG СТИСНЕННЯ.

Алгоритм JPEG є одним з найпопулярніших на сьогоднішній день методів стиснення зображень при обміні ними в мережі Інтернет. Його можна розділити на кілька етапів:

1. **Дискретизація.**

На цьому кроці дані пікселів перетворюються з колірного простору RGB в колірний простір YCbCr і виконується субдискретизація. Компонента Y являє собою інтенсивність, а U і V – кольоровість.

2. **Дискретне косинусне перетворення.**

Далі зображення JPEG стискаються в блоки 8x8 пікселів, які називаються одиницями даних. Дискретне косинусне перетворення перетворює одиниці даних в суму косинусних функцій.

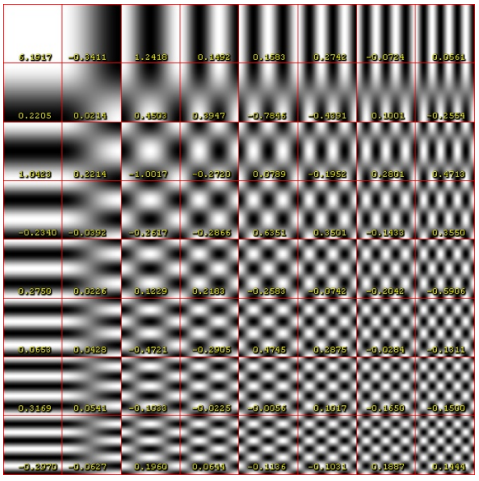


Рис. 1 – Зразок матриці частотних коефіцієнтів DCT

Графічне зображення можна розглядати як сукупність просторових хвиль, причому осі X і Y збігаються з шириною і висотою картинки, а по осі Z відкладається значення кольору відповідного пікселя зображення. Дискретне косинусне перетворення дозволяє переходити від просторового уявлення картинки до її спектрального подання і назад. Впливаючи на спектральне подання картинки, що складається з «гармонік», тобто, відкидаючи найменш значущі з них, можна балансувати між якістю відтворення і ступенем стиснення. У отриманій матриці коефіцієнтів низькочастотні компоненти розташовані ближче до лівого верхнього кута, а високочастотні – справа і знизу (рис. 1). Це важливо тому, що більшість графічних образів на екрані комп'ютера складається з низькочастотної інформації. Високочастотні компоненти не так важливі для передачі зображення.

Таким чином, дискретне косинусне перетворення дозволяє визначити, яку частину інформації можна безболісно викинути, не вносячи серйозних спотворень в картинку.

3. Квантування.

Після розрахунку ДКП наступний крок включає пошук і відкидання коефіцієнтів, внесок яких у формування зображення мінімальний. Для вирішення цього завдання стандарт JPEG визначає простий механізм іменований квантуванням. Щоб виконати квантування коефіцієнтів ДКП, необхідно розділити їх на конкретне значення (коефіцієнт квантування) і округлити результат до найближчого цілого числа. Чим більше коефіцієнт квантування, тим більше даних втрачається, оскільки реальне DCT-значення представляється все менш і менш точно.

Кожна з 64 позицій вихідного блоку ДКП має власний коефіцієнт квантування. Причому терми більшого порядку квантуються з більшим коефіцієнтом, ніж терми меншого порядку.

АЛГОРИТМ ВБУДОВУВАННЯ ДАНИХ.

Запропонована технологія основана на методах цифрового маркування, що вбудовують цифровий водяний знак (ЦВЗ) в частотну область зображення, використовуючи ортогональні перетворення для декомпозиції зображення-контейнера і перерозподілу його енергії [1–3]. Але, на відміну від цифрового маркування, де метою є перевірка наявності конкретного ЦВЗ у контейнері, даний метод дозволяє записати та зчитати з зображення дані вільного характеру.

Основне зображення буде перетворено з колірного простору RGB в колірний простір YCbCr. Хоча зорова система людини більш чутлива до змін

яскравості, ніж до змін кольоровості, проте канал яскравості (Y) основного зображення розглядається для впровадження даних, оскільки стиснення JPEG відкидає великий обсяг інформації про кольоровості під час її субдискретизації.

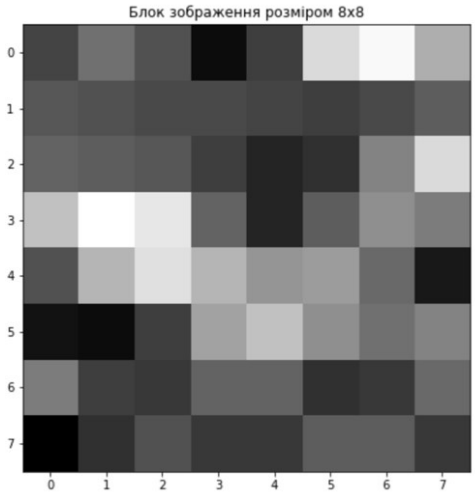


Рис. 2 – Блок компоненти яскравості зображення розміром 8x8

Для збільшення стійкості до JPEG-стиску кожен трансформований блок піддається квантуванню за допомогою стандартної таблиці квантування, що використовується при JPEG-стиску. На рисунку 4 червоним кольором позначені положення низькочастотних коефіцієнтів, використовуваних для вбудовування даних.

DC	0,1	0,2
1,0	1,1	1,2
2,0	2,1	

Рис. 4 – Положення модифікованих коефіцієнтів ДКП

Вибрані коефіцієнти, з урахуванням проаналізованої літератури, найбільш оптимальні для даної схеми. Внесення змін до коефіцієнтів C(0,1), C(1,0) і C(1,1) призведе до сильної деградації зображення. Модифікація коефіцієнтів C(0,3), C(1,2), C(2,1) і C(3,0) при їх використанні в даному алгоритмі зробить факт впровадження даних вразливим до статистичних методів виявлення.

На початковому етапі до вихідного повідомлення додається стоп-символ, що сигналізує про закінчення повідомлення при отриманні даних. Використання стоп-символу дозволяє повністю автоматизувати процес кодування та відновлення. Так, програма-декодер, виявивши стоп-символ, вважає, що витяг повідомлення закінчено і надає чистий висновок користувачеві.

Далі компонента яскравості зображення ділиться на ряд непересічних блоків розміром 8x8, кожен з яких піддається двовимірному ДКП, як наведено на рисунках 2 і 3.

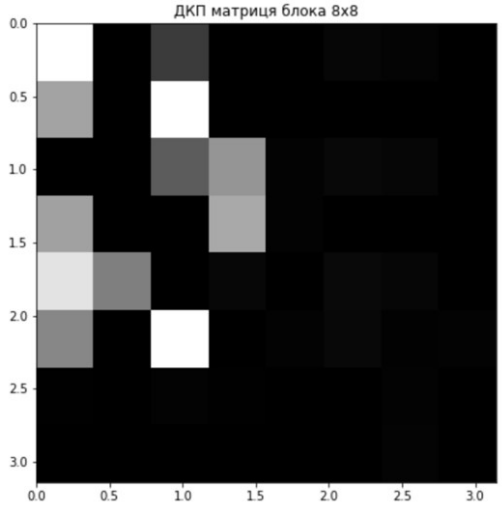


Рис. 3 – ДКП матриця блоку компоненти яскравості зображення розміром 8x8

Оригінал тексту разом із стоп-символом посимвольно перекладається в числову послідовність, де кожному числу відповідає номер відповідного символу в таблиці ASCII. Після цього кожне число переводиться в двійкову систему, отримуючи, таким чином, двійкову послідовність, яка буде показувати вихідне повідомлення, по вісім біт на кожен символ. Наприклад, якщо вихідне повідомлення звучить як «hello», а стоп-символом обрано «&», то результат буде таким:

1) в кінець повідомлення «hello» додається стоп-символ «&», отримуючи в результаті «hello&»;

2) «hello&», згідно з таблицею ASCII, перекладається в список чисел [104, 101, 108, 108, 111, 38];

3) ця послідовність, в свою чергу, перекладається в двійкову систему числення: [01101000, 01100101, 01101100, 01101100, 01101111, 00100110];

4) отримана двійкова послідовність вбудовується в зображення, як описано далі.

Далі здійснюється безпосереднє впровадження даних. Кожен біт повідомлення повинен бути впроваджений в один з двох зазначених коефіцієнтів ДКП, отримуючи в результаті по два біти на кожен блок 8x8. Як описувалося вище, ці коефіцієнти є найоптимальнішим варіантом.

Нарешті, обчислюється зворотне ДКП для перекладу зображення з частотної області назад в просторову. Цей крок є фінальним і в результаті видає зображення, дуже наближене до вихідного, але маюче вбудовані в нього дані. Даний алгоритм, на думку автора, реалізує кращі особливості частотних

методів ЦВЗ, балансуючи між стійкістю до стегоаналізу, складності реалізації, місткістю контейнера і стійкістю до стиснення з втратами, віддаючи перевагу останньому. Однак, залишається відкритим питання як саме вбудувати біт повідомлення в значення низькочастотного коефіцієнта так, щоб його можна було витягти після стиснення і при цьому залишалася б можливість корекції помилки. Для вирішення цієї проблеми пропонується використовувати принцип математичного залишку [4]. Алгоритм перетворює вихідне значення коефіцієнта ДКП (C) на модифіковане (C*), що належить певному діапазону, який можна коригувати для балансування між стійкістю та непомітністю. Процес вилучення даних з контейнера дуже схожий на процедуру їх вбудовування. Він є досить простим і не вимагає наявності вихідного зображення. Варто звернути увагу, що процедура вилучення даних приймає лише два параметри: модифікований ДКП коефіцієнт, в який були занесені дані, і модуль M. В загальних рисах, алгоритм наступний:

1) конвертація зображення в формат YCbCr і витяг компоненти яскравості;

2) поділ компоненти яскравості на непересічні блоки 8x8 і застосування до кожного і них двовимірного ДКП;

3) витяг біт вбудованого тексту відповідно до формули [4];

4) групування витягнутих біт і переведення їх у відповідний символ таблиці ASCII;

5) якщо поточний символ – стоп-символ, витяг повідомлення закінчено.

Зазначений алгоритм слід повторювати до виявлення стоп-символу, або до кінця контейнера. В останньому випадку вважається що контейнер або не містить повідомлення, або воно було істотно пошкоджено. Додатково замість стоп-символу можна використовувати стоп-інтервал, що дозволить збільшити можливості корекції помилки.

Для проведення наукового експерименту було вибрано частину зображення, значення яскравості і ДКП коефіцієнтів якої наведені на рисунках 5 та 6.

18.0	25.0	20.0	9.0	17.0	42.0	47.0	35.0
21.0	20.0	19.0	19.0	18.0	17.0	19.0	22.0
23.0	22.0	21.0	17.0	13.0	15.0	28.0	42.0
38.0	48.0	44.0	23.0	13.0	22.0	30.0	27.0
20.0	36.0	43.0	36.0	31.0	32.0	24.0	11.0
10.0	9.0	17.0	33.0	38.0	30.0	25.0	28.0
27.0	17.0	16.0	23.0	23.0	15.0	16.0	24.0
7.0	15.0	20.0	16.0	16.0	22.0	22.0	16.0

Рис. 5 – Значення яскравості 8x8 блоку зображення

189.0	-9.2	4.5	-6.9	-10.5	0.5	0.3	-0.0
12.3	-5.3	23.4	-0.3	-11.6	-0.1	0.0	-0.5
-25.1	-24.0	7.0	11.3	0.2	0.6	0.5	-0.2
12.2	-13.5	-19.7	12.8	0.3	-0.4	-0.2	-0.9
17.2	9.6	-0.6	0.6	-29.2	0.7	0.5	-0.4
10.3	0.1	23.3	0.0	0.3	0.6	0.2	0.3
0.1	-27.3	0.2	0.1	-0.1	-0.2	0.3	-0.2
-0.1	-0.5	-0.3	-0.6	-0.1	-0.1	0.3	-0.0

Рис. 6 – ДКП коефіцієнти 8x8 блоку зображення

Нехай послідовність, яку необхідно впровадити в зображення, виглядає як [1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1]. Перші два елементи – [1, 0] будуть вбудовані в відповідні ДКП коефіцієнти, наведені на рисунку 2.3 за вказаним правилом. Таким чином, біт «1» буде вбудований в значення -25.1, а біт «0» – в значення 4.5. На рисунку 7 показаний модифікований ДКП блок із зазначеними позиціями цільових коефіцієнтів.

189.0	-9.2	4.0	-6.9	-10.5	0.5	0.3	-0.0
12.3	-5.3	23.4	-0.3	-11.6	-0.1	0.0	-0.5
-31.0	-24.0	7.0	11.3	0.2	0.6	0.5	-0.2
12.2	-13.5	-19.7	12.8	0.3	-0.4	-0.2	-0.9
17.2	9.6	-0.6	0.6	-29.2	0.7	0.5	-0.4
10.3	0.1	23.3	0.0	0.3	0.6	0.2	0.3
0.1	-27.3	0.2	0.1	-0.1	-0.2	0.3	-0.2
-0.1	-0.5	-0.3	-0.6	-0.1	-0.1	0.3	-0.0

Рис. 7 – ДКП коефіцієнти 8x8 блоку зображення

ТЕОРЕТИЧНА СКЛАДОВА ДОСЛІДЖЕННЯ.

Описаний в попередньому розділі алгоритм є досить стійким до стиснення з втратами, але нестійким до такого типу атаки як несанкціонований витяг даних. Якщо третя сторона визначить алгоритм, використаний для впровадження даних, вона зможе безперешкодно отримати їх. Для забезпечення стійкості до подібних атак вихідні дані слід попередньо зашифрувати, враховуючи, що внаслідок стиснення з втратами, дані можуть бути відновлені лише частково.

З урахуванням цієї вимоги, має сенс вивчити можливість використання шифрів підстановки. У загальному випадку, шифр підстановки – це метод шифрування, в якому елементи вихідного відкритого тексту замінюються зашифрованим текстом відповідно до деякого правила.

На рисунку 8 показано, як слово «HELLO» було зашифровано в рядок «URYYB» з використанням додаткового алфавіту.

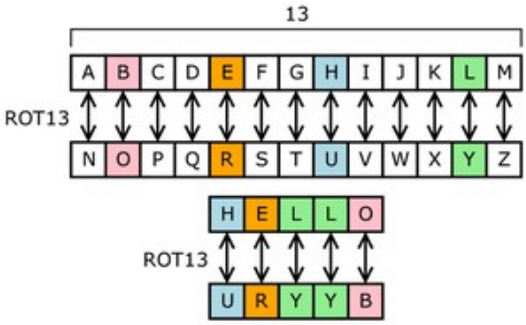


Рис. 8 – Застосування моноалфавітного шифру підстановки

Однак, у даного методу є серйозний недолік – його досить просто зламати використовуючи так званий частотний аналіз [5] або, в більш серйозних випадках, генетичні алгоритми [6].

Частотний аналіз передбачає, що частота появи заданої літери алфавіту в досить довгих текстах одна і та ж для різних текстів однієї мови. При цьому, в

разі моноалфавітного шифрування, якщо в шифротекста буде символ з аналогічною ймовірністю появи, то можна припустити, що він і є зазначеної зашифрованою буквою. Так, на рисунку 9 наведено розкид частоти використання букв англійського алфавіту.

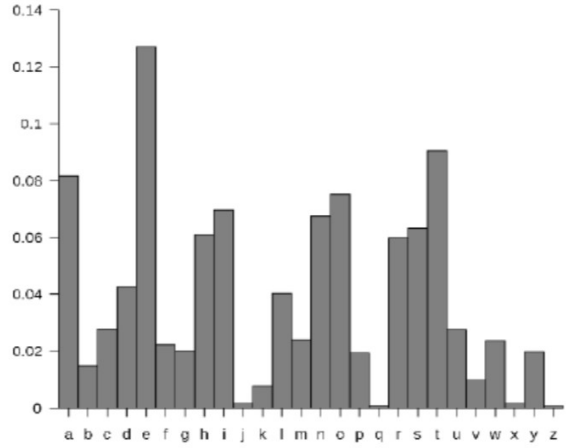


Рис. 9 – Частотний розподіл букв англійського алфавіту

Проаналізувавши частотний розподіл зашифрованого тексту і зіставивши його з типовим для даної мови, можна досить просто розшифрувати такий текст. Для того щоб підвищити стійкість алгоритму до розшифровки, пропонується використовувати поліалфавітний шифр підстановки, що є сукупністю шифрів простої заміни (моноалфавитних шифрів), які використовуються для шифрування чергового символу відкритого тексту згідно деякому правилу. Поліалфавітний шифр куди менш схильний до частотного аналізу і спробам злому з використанням генетичних алгоритмів. Як показано на рисунку 3, два однакових символи вихідного тексту дають різні символи зашифрованого тексту при використанні поліалфавітного шифру.

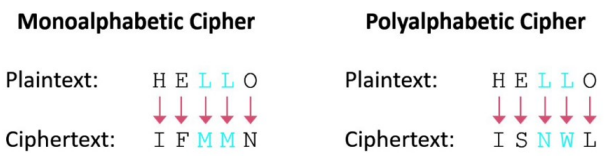


Рис. 10 – Порівняння зашифрованих різними методами текстів

Це означає, що частотний аналіз не дасть результатів при спробі злому поліалфавітного шифру. Подібне завдання є досить важким і тим воно важче, чим менше зв'язку між вихідним текстом і зашифрованим. Тому, для додаткової надійності, пропонується додати в алгоритм можливість введення призначеного для користувача секретного ключа і здійснення операції XOR між ним і вихідним текстом. Оскільки операція XOR оборотна, текст можна буде розшифрувати за допомогою того ж ключа.

Розглянемо фінальний запропонований варіант шифрування. Нехай дано кілька вихідних алфавітів, кожен з яких є випадковою перестановкою символів в таблиці ASCII. Також дано вихідний текст, а саме: «keep calm and study hard» і секретний ключ: «lemon». Unicode значення отриманих алфавітів наведені на рисунку 11.

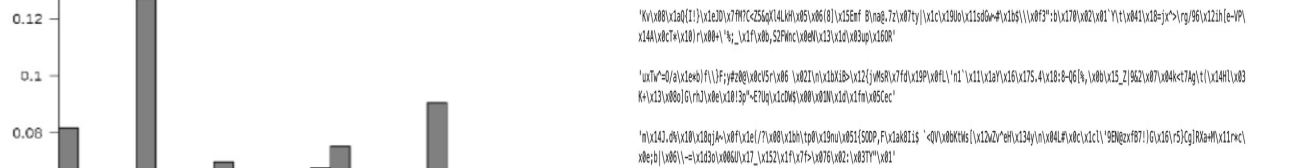


Рис. 11 – Unicode значення алфавітів, отримані в результаті трьох випадкових перестановок символів таблиці ASCII

Першим кроком виконується XOR кодування вихідного тексту з секретним ключем. В даному випадку, перший символ вихідного тексту «k» буде закодований з першим символом секретного ключа «l», другий символ «e» – з другим символом ключа «e» і так далі. Отримана в результаті послідовність шифрується за допомогою обраних алфавітів. Так, перший символ послідовності замінюється на відповідний символ першого алфавіту, другий символ – на символ другого алфавіту і так далі. Всі алфавіти використовуються один за одним по черзі і після останнього процес переходить назад до першого. Отримана в результаті послідовність виглядає наступним чином: «'J | ## \ rv7 \ x1enYDE \ x12 \ r \ x0b \ x7f_S6 \ r 7SS'». Після підстановки Unicode символів і перекладу послідовності в двійкову систему, отримуємо послідовність, наведену на рисунку 12.

```
01001010 01111100 00100011 00100011
00001101 01110110 00110111 00011110
01101110 01011001 01000100 01000101
00010010 00001101 00001011 01111111
01011111 01010011 00110110 00001101
00100000 00110111 01010011 01010011
```

Рис. 12 – Двійкове подання зашифрованого тексту

Отримана таким чином двійкова структура розбивається на пари сусідніх бітів і переноситься в низькочастотні області цільового зображення, як описано вище.

ВИСНОВКИ ТА АНАЛІЗ ЕФЕКТИВНОСТІ РОЗРОБЛЕНОГО АЛГОРИТМА.

Для проведення аналізу стійкості алгоритму до JPEG стиснення в вихідне зображення було вбудовано повідомлення «Keep calm and study hard» з використанням секретного ключа «lemon», потім вихідне зображення було стиснене з різним коефіцієнтом стиснення і проведено порівняння відновленого згодом тексту з вихідним. Результати аналізу наведені на рисунку 13.

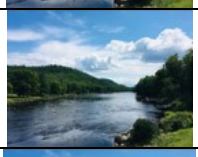
Зображення	Коефіцієнт стискання	Відновлений текст
	1.0	Keep calm and study hard
	0.9	Keep calm and study hard
	0.8	Keep c lm and study hcrd
	0.6	#eep cs\m and tu%y hard
	0.4	P galm7aKN 4s@ hard

Рис. 13 – Аналіз стійкості алгоритму з стиску з втратами

Можна зробити висновок, що алгоритм є досить стійким до стиснення з втратами при використанні коефіцієнта стиснення не менше 0,6. Незважаючи на частково пошкоджений внаслідок стиснення текст, використання поліалфавітного шифру підстановки дозволило розшифрувати його на прийнятному рівні, що є великою перевагою запропонованого методу. Даний результат збігається з можливостями проаналізованих методів вбудовування ЦВЗ в частотну область зображення, на основі яких було розроблено алгоритм.

Таким чином, у цій статті було розглянуто стеганографічний алгоритм прихованої передачі інформації в растрових зображеннях, що є досить стійким до стиснення з втратами і атаками на контейнер. Практична цінність представленої роботи полягає в доведенні отриманих наукових результатів до конкретного алгоритму, який може бути використаний як складова комплексних систем захисту інформації будь-якого підприємства, установи та може бути використана для навчання студентів [7–20] за представленими прикладами.

Список літератури

1. Грибунин В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, В. И. Туринцев. – М.: СОЛОН-Пресс, 2002. – 272с.
2. Конахович Г. Ф. Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю. Пузыренко. – К.: «МК-Пресс», 2006. – 288 с.
3. Elshoura, S. M. A secure high capacity full-gray-scale-level multi-image information hiding and secret image authentication scheme via Tchebichef moments / S. M. Elshoura, D. B. Megherbi // Signal Processing: Image Communication. 2013. – Vol. 28, pp. 531–552.
4. Shinfeng D. Lin, Shih-Chieh Shie, and Jim Yi Guo. 2009. Improving the Robustness of DCT-Based Image Watermarking Against JPEG Compression. Elsevier, Journal of Computer Standard and Interfaces Volume 32, Issues 1-2, pp. 54–60.
5. Ronak Dedhia, Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for more Secure Communication, pp. 2–3.
6. Dalal Alsaady, Safaa Omran. USING GENETIC ALGORITHM TO CRYPTANALYSE A SIMPLE SUBSTITUTION CIPHER, pp. 13–26.
7. Бухкало С.І. Особливості розробки об'єктів інтелектуальної власності зі студентами. XXV Межд. н-практ. конф. «Информационные технологии: наука, техника, технология, образование, здоровье» (MicroCAD-2018) 17-19 мая 2018. Х.: Ч. II, с. 201.
8. Бухкало С.І. Удосконалювання методів оцінки знань студентів вищих навчальних закладів. Вісник НТУ «ХПІ». Х.: НТУ «ХПІ». 2014, № 16, с. 3–11.
9. Bukhkalo S.I., Ageicheva A.O., Iglin S.P., Hlavcheva Yu. N., Miroshnichenko N.N., Zipunnikov M.M., Olkhovska V.O. Innovative complex projects'2018/2019 realization in the examples and tasks / Вісник НТУ «ХПІ». 2019. – № 15(1340). – С. 80–88. doi: 10.20998/2220-4784.2019.15.14
10. Бухкало С.И., Гардер С.Е. и др. Регулирование эффективности ресурсо- и энергосбережения на комплексных предприятиях по переработке отходов // Вісник НТУ «ХПІ». 2012. – № 10. – с. 72–80.
11. Бухкало С.І. Загальна технологія харчових виробництв у прикладах і задачах (приклади та тести з технології крохмалю). 2-ге вид. доп.: ч. 2, [текст] підручник з грифом МОН / С. І. Бухкало – К.: ЦНЛ, 2019. – 108 с.
12. Бухкало С.І. Основні складові комплексних підприємств енергетичного міксу. Вісник НТУ «ХПІ». 2015. № 7 (1116), с. 103–108.
13. Ольховська В.О., Кравченко О.С., Бухкало С.І. Складові алгоритму пошуку раціональних закономірностей роботи обладнання. Інформаційні технології: наука, техніка, технологія, освіта, здоров'я: тези доповідей XXVIII міжн. н/практ.конф. (MicroCAD-2020) Ч. II. / за ред. проф. Сокола Є.І. – Харків: НТУ «ХПІ». С. 250.
14. Кравченко О.С. Загальна технологія системи технічного зору в прикладах і задачах. Вісник НТУ «ХПІ». Х.: НТУ «ХПІ». 2019, № 21(1346), с. 44–51.
15. Сирку М.А., Бухкало С.І., Іглін С.П, Мірошніченко Н.М. та ін. Питання комплексного визначення властивостей сировини у межах курсових проектів. Інформаційні технології: наука, техніка, технологія, освіта, здоров'я: тези доповідей XXVII міжн. н-пр. конф. MicroCAD-2019, 15-17 травня 2019р. Ч. II / за ред. проф. Сокола Є.І. Х :.НТУ «ХПІ». 342 с.
16. Бухкало С.И., Гардер С.Е., Химич О.Ю. и др. Применение математического моделирования для комплексных предприятий по переработке отходов. Вісник НТУ «ХПІ». 2012, № 10, с. 74–78.
17. Бухкало С.І. Деякі моделі процесів хімічного спінювання вторинного поліетилену. Вісник НТУ «ХПІ». 2017. № 18 (1240), с. 35–45.
18. Бухкало С.І. Основні складові комплексних підприємств енергетичного міксу. Вісник НТУ «ХПІ». 2015. № 7 (1116), с. 103–108
19. Bukhkalo S.I., Ageicheva A.O., Iglin S.P. Innovative complex projects'2018/2019 realization in the examples and tasks. Вісник НТУ «ХПІ». – Х.: НТУ «ХПІ», 2019. – № 15(1340), с. 80–88. doi: 10.20998/2220-4784.2019.15.14
20. Бухкало С.І. Синергетичні моделі для екологічно-безпечних процесів ідентифікації-класифікації вторинних полімерів. Вісник НТУ «ХПІ». – Х.: НТУ «ХПІ», 2018. – № 18(1294), с. 36–44.

Bibliography (transliterated)

1. Gribunin V. G. Cifrovaja steganografija / V. G. Gribunin, I. N. Okov, V. I. Turincev. M.: SOLON-Press, 2002. – 272 p.

2. Konahovich G. F. Komp'juternaja steganografija. Teorija i praktika / G. F. Konahovich, A. Ju. Puzyrenko. – K.: «MK-Press», 2006. – 288 p.
3. Elshoura, S. M. A secure high capacity full-gray-scale-level multi-image information hiding and secret image authentication scheme via Tchebichef moments / S. M. Elshoura, D. B. Megherbi // Signal Processing: Image Communication. 2013. – Vol.28, pp. 531–552.
4. Shinfeng D. Lin, Shih-Chieh Shie, and Jim Yi Guo. 2009. Improving the Robustness of DCT-Based Image Watermarking Against JPEG Compression. Elsevier, Journal of Computer Standard and Interfaces Volume 32, Issues 1-2, pp. 54–60.
5. Ronak Dedhia, Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for more Secure Communication, pp. 2–3.
6. Dalal Alsaady, Safaa Omran. USING GENETIC ALGORITHM TO CRYPTANALYSE A SIMPLE SUBSTITUTION CIPHER, pp. 13–26.
7. Bukhkalo S.I. Osoblivosti rozrobki ob'ektiv intelektual'noï vlasnosti zi studentami. XXV Mezhd. n-prakt. konf. «Informacionnye tehnologii: nauka, tehnika, tehnologija, obrazovanie, zdorov'e» (MicroCAD-2018) Kh.: II, p. 201.
8. Bukhkalo S.I. Udoskonaljuvannja metodiv ocinki znan' studentiv vishhih navchal'nih zakladiv. Visnik NTU «KhPI». Kh.: NTU «KhPI». 2014, № 16, pp. 3–11.
9. Bukhkalo S.I., Ageicheva A.O., Iglin S.P., Hlavcheva Yu. N., Miroshnichenko N.N., Zipunnikov M.M., Olkhovska V.O. Innovative complex projects'2018/2019 realization in the examples and tasks / Visnik NTU «KhPI». 2019. – № 15(1340), pp. 80–88. doi: 10.20998/2220-4784.2019.15.14
10. Bukhkalo S.I., Garder S.E., Ol'hovskaja O.I. Regulirovanie jeffektivnosti resurso- i jenergosberezhenija na kompleksnyh predprijatijah po pererabotke othodov/Visnik NTU «KhPI». Kh.: NTU «KhPI». 2012. № 10, pp. 72–80.
11. Bukhkalo S.I. Zagal'na tehnologija harchovih virobnictv u prikladah i zadachah (prikladi ta testi z tehnologiï krohmalju). 2-ge vid. dop.: ch. 2, [tekst] pidruchnik z grifom MON / S. I. Bukhkalo – K.: Centr navchal'noï literaturi, 2019. – 108 p.
12. Bukhkalo S.I. Osnovni skladovi kompleksnih pidpricmstv energetichnogo miksu. Visnik NTU «KhPI». 2015. № 7 (1116), pp. 103–108.
13. Ol'hovs'ka V.O., Kravchenko O.S., Buhkalo S.I. Skladovi algoritmu poshuku racional'nih zakonomirnostej roboti obladnannja. Informacijni tehnologiï: nauka, tehnika, tehnologija, osvita, zdorov'ja: tezi XXVIII mizhn. n/prakt.konf. (MicroCAD-2020) NTU «KhPI», p. 250.
14. Kravchenko O.S. Zagal'na tehnologija sistemi tehnichnogo zoru v prikladah i zadachah. Visnik NTU «KhPI». Kh.: NTU «KhPI». 2019, № 21(1346), pp. 44–51.
15. Sirku M.A., Bukhkalo S.I., Iglin S.P, Miroshnichenko N.M. ta in. Pitannja kompleksnogo viznachennja vlastivostej sirovini u mezhah kursovih proektiv. Informacijni tehnologiï: nauka, tehnika, tehnologija, osvita, zdorov'ja: tezi dopovidej XXVII mizhn. n-pr. konf. MicroCAD-2019, Ch. II/za red. prof. Sokola Є.I. Kh.: NTU «KhPI», p. 342.
16. Bukhkalo S.I., Garder S.E. Primenenie matematicheskogo modelirovanija dlja kompleksnyh predprijatij po pererabotke othodov. Visnik NTU «KhPI». 2012, № 10, pp. 74–78.
17. Bukhkalo S.I. Dejaki modeli procesiv himichnogo spinjuvannja vtorinnogo polietilenu. Visnik NTU «KhPI». 2017. No. 18 (1240), pp. 35–45.
18. Bukhkalo S.I. Osnovni skladovi kompleksnih pidpricmstv energetichnogo miksu. Visnik NTU «KhPI». 2015. No. 7 (1116), pp. 103–108
19. Bukhkalo S.I., Ageicheva A.O., Iglin S.P. Innovative complex projects'2018/2019 realization in the examples and tasks. Visnik NTU «KhPI». 2019. – No. 15(1340), pp. 80–88. doi: 10.20998/2220-4784.2019.15.14
20. Bukhkalo S.I. Sinergetichni modeli dlja ekologichno-bezpechnih procesiv identifikacij-klasifikacij vtorinnih polimeriv. Visnik NTU «KhPI». 2018. – № 18, pp. 36–44.

Надійшла (received) 19.11.2021

Відомості про авторів / Сведения об авторах / About the Authors

Кравченко Олександр Сергійович (Кравченко Александр Сергеевич, Kravchenko Oleksandr Serhijovych) – аспірант, кафедра Комп'ютерних наук і аналізу даних, факультет Комп'ютерних наук, НТУ «ХПІ», м. Харків, Україна; e-mail: askraff@gmail.com.

O. S. KRAVCHENKO

GENERAL TECHNOLOGY OF ENCRYPTION AND INTEGRATION OF DATA IN A PATTERN OF A PICTURE OF IMAGES THAT IS RESISTANT TO JPEG COMPRESSION

The object of the thesis is the use of steganographic methods for organizing a covert communication channel in a public channel, providing resistance to lossy compression. The aim of the thesis is to develop an algorithm for embedding data into bitmap images that is resistant to JPEG compression and attacks on the container. In this thesis, the features of the JPEG algorithm are investigated, steganographic methods of information protection are analyzed, and a steganographic algorithm is designed that is resistant to JPEG compression and attacks on the container. Additional security is provided by the polyalphabetic substitution cipher and user secret key used to encrypt the original message. The algorithm was developed using the Python 3 programming language, the NumPy, SciPy, MatPlotLib libraries and the Jupyter Lab package. The task was completed using standard mathematical and statistical methods and tools of the high-level programming language Python 3.

Keywords*:* steganography, cryptography, JPEG algorithm, steganographic container stability, data embedding in raster images, stegoanalysis.

А. С. КРАВЧЕНКО

ОБЩАЯ ТЕХНОЛОГИЯ ШИФРОВАНИЯ И ВСТРАИВАНИЯ ДАННЫХ В РАСТРОВЫХ ИЗОБРАЖЕНИЯХ, УСТОЙЧИВЫХ К СЖИМАНИЮ JPEG

Объектом исследования представленной статьи являются стеганографические методы организации скрытого канала связи в канале общего пользования, обеспечивающие устойчивость к сжатию с потерями. Цель работы – разработка алгоритма встраивания данных в растровые изображения, устойчивого к сжатию JPEG и атакам на контейнер. В работе исследованы особенности работы алгоритма JPEG, проанализированы стеганографические методы защиты информации и построен стеганографический алгоритм, устойчивый к сжатию JPEG и атакам на контейнер. Дополнительную надежность обеспечивают полиалфавитный шифр подстановки и пользовательский секретный ключ, используемый для шифрования исходного сообщения. Алгоритм был разработан с помощью языка программирования Python 3, библиотек NumPy, SciPy, MatPlotLib и пакета Jupyter Lab. Задача была выполнена с помощью стандартных математических и статистических методов и средств высокоуровневого языка Python 3.

Ключевые слова: стеганография, криптография, JPEG алгоритм, устойчивость стеганографического контейнера, встраивание данных в растровые изображения, стегоанализ.