УДК 004.056.5 **Козіна М.О., Папковська О.Б., Логінова Н.І., Козін О.Б.**

СТЕГАНОАЛГОРИТМ, ЩО ВИКОРИСТОВУЄ СИНГУЛЯРНЕ РОЗКЛАДАННЯ МАТРИЦІ КОНТЕЙНЕРА

Однією з найпоширеніших на сьогоднішній день атак, яким піддаються системи прихованої передачі цифрових даних в стеганографії – атака стисненням. У роботі пропонується новий стеганоалгоритм на основі сингулярного розкладання матриці контейнера. Ефективність розробленого стеганоалгоритму оцінювалась візуальною оцінкою якості; ступенем забезпечення надійності сприйняття формованого стеганоповідомлення; у тому числі і після атаки стисненням з різним ступенем стисненню. Це не призводило до порушення надійності сприйняття та дало високі результати на обраних вибірках.

Ключові слова: атака стисненням, сингулярне розкладання, максимальні сингулярні числа, стеганоалгоритм, стеганографія.

1. Вступ

Постанова задачі. Розвиток інформаційних технологій дав поштовх до розробки нових сучасних методів, призначених для організації безпеки передачі даних каналами телекомунікацій, що на сьогоднішній день набуло широке застосування у комерційних цілях. Перспективним напрямком організації безпеки інформації у сучасних системах і мережах є цифрова стеганографія [1-3].

Популярність атак стисненням пов'язана зараз з широким розповсюдженням алгоритмів стиснення графічних файлів з втратами для зберігання і пересилки інформації, що не приваблює увагу до цих файлів адресатів не тільки при використанні прихованої, але і відкритої передачі даних. Наприклад, при поширенні інформації в соціальних мережах, захист інформації та забезпечення її достовірності є невирішеними питаннями на сьогодні [4]. У зв'язку з цим до сучасних стеганографічних методів і алгоритмів пред'являється обов'язкова вимога стійкості до впливу в каналі зв'язку.

Сьогодні стеганографія дозволяє не тільки успішно вирішувати основну задачу – приховано передавати інформацію, але і цілий ряд інших актуальних завдань. Наприклад – вбудовування прихованої інформації з метою захисту авторських прав на інтелектуальну власність, представлену в цифровому вигляді [1]. Ця прихована інформація називається цифровим водяним знаком (ЦВЗ). ЦВЗ є спеціальна позначка, яка містить спеціальну інформацію, однозначно підтверджує авторство або права на комерційне використання об'єкта, що захищається. Він непомітно впроваджується в зображення або інший сигнал з метою тим чи іншим чином контролювати його використання. Дані, які містять приховане повідомлення, можуть також зазнати випадкових перешкод або навмисних атак.

На сьогоднішній день, цифрове зображення (ЦЗ) дуже часто використовується в якості контейнера в стеганографії. Одна з причин полягає в можливості змін матриці зображення в процесі стеганоперетворень (СП), які не призводять до порушень надійності сприйняття формованого стеганоповідомлення. В цій роботі в якості контейнера розглядається цифрове зображення.

Метою даної роботи *є* розробка нового стеганоалгоритму на основі сингулярного розкладання матриці контейнера та дослідження його ефективності на основі практичного експерименту з визначення надійності сприйняття сформованого стеганоповідомлення запропонованим в роботі алгоритмом після атак стисненням**.**

Аналіз предметної області. Методи приховування даних у просторовій області зображення є нестійкими до більшості з відомих видів спотворень, наприклад до стиснення з втратами. Таким чином, найбільший інтерес в області цифрових зображень представляють методи вбудовування інформації в зображення, де відбувається стиснення з втратами (популярний формат JPEG). Для вбудовування

інформації використовується просторова або частотна область. Методи, які використовують для приховування даних частотну область, є більш стійкі до різних можливих зовнішніх впливів на зображення-контейнер [1].

У науковій роботі [5] був розроблений алгоритм перевірки цілісності цифрового кольорового зображення-контейнера з урахуванням можливості виходу за межі діапазону значень яскравості пікселів в матриці зображення на етапі кодування. Проаналізовано розбиття матриці зображення на блоки різного розміру, обчислення частотних коефіцієнтів дискретного косинус перетворення для блоків розглянутих розмірів.

В роботі [6] автори представили стеганометод, який організовує прихований канал зв'язку шляхом вбудовування додаткової інформації в частотну область. Пропонований метод вкладення додаткової інформації в коефіцієнти дискретних перетворень Хартлі. Він має симетрію формул прямого і зворотного перетворення, тому він забезпечує високу обчислювальну ефективність при обробці дійсного типу даних.

В роботі [7] представлені достатні умови стійкості стеганометодів і стеганоалгоритмів до стиснення, в тому числі зі значними коефіцієнтами, які не залежать від того, яка область цифрового зображення-контейнера – просторова або область перетворення використовується для вбудови додаткової інформації.

Отримання цих умов стало поштовхом до подальшого розвитку загального підходу до аналізу стану і технології функціонування інформаційних систем, заснованого на матричному аналізі та теорії збурень, і адаптації його для вирішення завдань стеганографії [8].

Відповідно до отриманих достатніми умов у роботі, стійкість до стиснення стеганоалгоритма буде забезпечена в разі виконання певних умов при проведенні процесу впровадження інформації у контейнер. А саме, потрібно, щоб при формальному поданні результату вбудови у вигляді сукупності збурень сингулярних чисел (СНЧ) і / або сингулярних векторів (СНВ) блоків матриці контейнера, отриманих в результаті стандартного розбиття, ці сукупності містили збурення максимальних СНЧ і / або СНВ, що відповідають максимальним СНЧ блоків.

На основі описаних достатніх умов отриманих раніше, автором роботи [9] був розроблений стеганографічний алгоритм, який є стійким до атаки одноразового і дворазового стиснення. Також він має малу обчислювальну складність – поліноміального ступеня 2. Характеристики розробленого алгоритму лише залежать від формату використовуваного зображення-контейнера. За рахунок відсутності необхідності переходу в область перетворення контейнера при організації вбудови/декодування додаткової інформації підвищена ефективність розробленого стеганоалгоритму, у порівнянні з аналогом, що здійснює вбудову конфіденційної інформації в область сингулярного розкладання матриці контейнеру [9].

Однак ні первинний, ні вдосконалений стеганоалгоритм, запропонований автором вищезгаданої роботи не забезпечує достатнє збереження надійності сприйняття і не дає одиничний коефіцієнт кореляції при збереженні стеганоповідомлення у форматі без втрат, що говорить, про значні збурення матриці при стеганоперетворенні.

Ще один сучасний стеганографічний алгоритм [10] запропонований авторами позиціонує себе як ефективний, виконує вимоги для побудови ефективного стеганоалгоритма, проте що стосується атаки стисненням - питання залишається відкритим.

У роботах [7,8] був використаний загальний підхід до аналізу стану і технології функціонування довільної інформаційної системи, заснований на теорії збурень і матричному аналізі. В силу цього, процес СП, незалежно від способу і області вбудови додаткової інформації і результату активних атакуючих дій, зокрема, стиснення, і т.д.,

формально може бути представлений як сукупність збурень сингулярних чисел (СНЧ) і/або сингулярних векторів (СНВ) відповідної матриці (матриць) контейнеру [7,8].

Авторами роботи [11] запропонована теоретична розробка стеганографічного методу, що використовує сингулярне розкладання матриці контейнера.

Результати робіт [7,8], покладені в основу теоретичних розробок пропонованого в даній роботі нового стеганометода. На базі розробленого стеганометода [11] пропонується стеганоалгоритм, ефективність якого буде оцінена і проаналізована в даній роботі.

2. Теоретична основа

Нехай F – m×n матриця контейнера. Загальна схема запропонованого стеганографічного алгоритму складається з трьох основних етапів. Спочатку проводимо попереднє розбиття матриці зображення F на непересічні блоки f стандартного розміру 8×8. Після цього для кожного блоку отримуємо сінгнулярне розкладання. Максимальні сингулярні числа отримують обурення у вигляді додаткової інформації в залежності від значення біта додаткової інформації, що не приводить до порушення надійності сприйняття сформованого стеганоповідомлення.

Для кожного блоку f проводимо побудову єдиного нормального сингулярного розкладання:

$$f = U\Sigma V, \quad (1)$$

де U, V – ортогональні матриці розміру 8×8, стовпці u_1, ..., u_8 матриці U - ліві СНВ,

лексикографічно позитивні (стовпці v_1, ..., v_8 матриці V називають правими СНВ матриці f); $\Sigma = \text{diag}(\sigma_1, ..., \sigma_8)$, $\sigma_1 \geq ... \geq \sigma_8 \geq 0$ – СНЧ.

Процес стиснення ЦЗ зробить певним чином збурення СНЧ матриць блоків. Оскільки сукупності СНЧ матриць ЦЗ в просторової і частотної областях збігаються, будь-які збурення СНЧ проявляться однаково для матриць блоків ЦЗ як у просторовій, так і у частотній області. Тому формалізація процесу СП у вигляді сукупності збурень СНЧ блоків не залежить від аналізованої області зображення (просторової, частотної), що є значущою перевагою обраного способу формального уявлення СП.

СНЧ матриці є добре обумовленими [12]. Найбільш яскраво особливості їх збурень при стисненні проявляються для найменших СНЧ матриці f. Значення найменших СНЧ блоків зображення, що зберігається в форматі з втратами, можна порівняти з похибкою округлення один з одним, що не характерно для блоків ЦІ, що зберігається без втрат. Крім того, характер поведінки найменших СНЧ (σ_6, σ_7, σ_8) блоків зображень з втратами якісно відрізняється від характеру СНЧ з тими ж номерами для блоків зображень, збережених без втрат: швидкість їх зміни в першому випадку значно менше аналогічних для другого випадку.

2.1. Пропонований алгоритм

Маємо F – m×n-матрицю – одну з колірних складових кольорового ЦЗ-контейнера довільного формату, для зберігання якого використана схема RGB.

В якості додаткової інформації виступає послідовність p_1, p_2, ... p_i, де $p_i \in \{0,1\}$, та i = 1,2, ..., t, де t = [M/8]·[N/8], [·] – ціла частина числа.

В алгоритмі введено таке позначення: T – параметр, значення якого пропонується покласти рівним другому сингулярному числу σ_2. Функція "roundn" – функція округлення числових значень до значення іншого параметра K. При здійсненні операції округлення K – розряд, до якого треба проводити округлення чисел, що залежить від значення сингулярного числа. При проведенні аналізу максимальних змін сингулярних чисел для довільних зображень пропонується параметр K вибрати між 10 і 100. Тобто проводити округлення до сотень в разі, якщо значення сингулярного числа не менше 100. Якщо ж значення сингулярного числа менше 100, то необхідно

проводити округлення до десятків. Наприклад, значення 98 після операції roundn (98,10) = 90.

Основні кроки пропонованого стеганографічного алгоритму, назвемо його А1, наступні.

Впровадження інформації

1. Матриця F розбивається на непересічні блоки f, розміру 8 × 8. Один блок розбиття використовується для впровадження 1 біта додаткової інформації.

2. Для кожного блоку f матриці F:

2.1 побудовано сингулярне розкладання для кожного блоку f (1);

2.2 якщо біт додаткової інформації $p = 0$,

тоді коригуємо максимальне значення СНЧ

$\overline{\sigma_1}$ = roundn (σ_1, K) + 1/4 · σ_2;

інакше (в разі якщо біт додаткової інформації $p = 1$)

$\overline{\sigma_1}$ = roundn (σ_1, K) + 3/4 · σ_2.

3. Повернення в просторову область. Для цього використовуємо сингулярне розкладання

$$f = U\bar{\Sigma}V^T,$$

де $\bar{\Sigma} = diag(\overline{\sigma_1}, \sigma_2, \ldots \sigma_8)$.

Декодування інформації

1. Матриця отриманого адресатом зображення $\bar{F}$ розбивається на блоки стандартним чином 8×8.

2. Для кожного блоку $\bar{f}$ матриці $\overline{F}$:

2.1 побудовано сингулярне розкладання

$$\bar{f} = \overline{U}\bar{\Sigma}\overline{V^T};$$

2.2 якщо ($\overline{\overline{\sigma 1}}$ – roundn ($\overline{\overline{\sigma 1}}$, K)) <1/2 · $\overline{\sigma 2}$ (Рис.1), тоді $\bar{p}$ = 0, інакше $\bar{p}$ = 1.

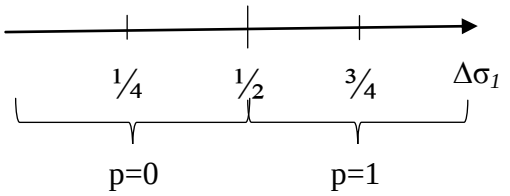

Рис. 1. Зміни максимального сингулярного числа $\Delta\sigma_1$

3. Апробація розробленого стеганоалгоритму

Ефективність розробленого стеганоалгоритму буде оцінюватися у такий спосіб:

– візуальною оцінкою якості;

– ступенем забезпечення надійності сприйняття формованого стеганоповідомлення;

– ступенем забезпечення надійності сприйняття формованого стеганоповідомлення після атаки стисненням з різним ступенем стиснення, що не призводити до порушення надійності сприйняття.

Одним з перших параметрів оцінки при побудові стеганографічних алгоритмів є оцінка надійності сприйняття цифрового зображення після впровадження додаткової інформації або ЦВЗ, тобто візуальна оцінка якості сформованого стеганографічного повідомлення. Візуальна оцінка не дала візуальних артефактів, що підтверджує практичний тест на вибірці з 50 зображень, які взяті випадковим чином, різних за контрастності, різкості, формату (с/без втрат) і іншими параметрами, на які приділяється увага при тестуванні стеганоалгоритмів. На рисунку 1 представлений приклад стеганоповідомлення.

Рис. 2. Приклад сформованого стеганоповідомлення з використанням пропонованого стеганоалгоритму A1

Зауважимо, що моделювання неідеального каналу зв'язку в силу специфіки даної задачі має сенс проводити за допомогою малих збурюючих дій, тому що в результаті будь-яких дій на стеганоповідомлення повинна зберегтись надійність сприйняття, інакше дії атакуючого будуть легко виявлені сторонами, які організовують прихований канал зв'язку. В якості малих збурюючих дій на канал зв'язку розглянуто стиснення з різними коефіцієнтами стиснення Q>70.

Практичний експеримент проводився у такий спосіб: у вибране довільне зображення проводилась вбудова додаткової інформації запропонованим у роботі стеганоалгоритмом, після цього отримане стеганоповідомлення зберігалося в форматі без втрат (TIF) або з втратами в форматі JPEG з різними коефіцієнтами стиснення Q.

Надійність сприйняття формованого стеганоповідомлення чисельно оцінюється стандартним чином за допомогою пікового відношення «сигнал-шум» PSNR. У відкритій пресі вважається надійність сприйняття стеганоповідомлення не порушена, якщо PSNR > 37Db. З таблиці 1 видно, що побудований стеганоалгоритм не приводить до порушення надійності сприйняття.

Таблиця 1

Оцінка надійності сприйняття (PSNR) формованого стеганоповідомлення запропонованим стеганоалгоритмом A1

Q / Алг.	TIF	100	90	80	70
A1	45	44,9	44,5	41	40,6

4. Висновки

У роботі автори представили новий стеганоалгоритм, що використовує сингулярне розкладання. Практичний експеримент показав високу надійність сприйняття сформованого стеганоповідомлення запропонованим в роботі алгоритмом. Проведено оцінки коефіцієнта надійності сприйняття запропонованих алгоритмом для формованого стеганоповідомлення без стиснення та після атаки стисненням з різним ступенем стиснення. В результаті обчислень для коефіцієнта PSNR отримана наступна оцінка: PSNR > 40 Db.

Список використаних джерел:

1. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н.Оков, И.В.Туринцев. — М.: СОЛОН-ПРЕСС, 2009. — С.272.

2 . Bergman, C. Unitary Embedding for Data Hiding with the SVD / C. Bergman, J. Davidson. // Proceedings of Security, Steganography, and Watermarking of Multimedia Contents VII, San Jose, CA, January 17, 2005. — Vol. 5681. — PP. 619–630.

3. Аграновский, А.В. Стеганография, цифровые водяные знаки и стеганоанализ / А.В. Аграновский, А.В.Балакин, В.Г. Грибунин, С.А.Сапожников. – М.: Вузовская книга, 2009. – С.220.

4. Мехед Д. Інформаційна безпека соціальних мережах. Методи поширення інформації в соціальних мережах / Д. Мехед. – Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип.2 (30), 2015. – С.14-18.

5. Козіна М.О., Кремінський В.Ю., Козін О.Б., Нджикє Амугу С.-М. Алгоритм перевірки цілісності цифрового зображення. // Сучасний захист інформації. – 2016 . – №4. – С. 41 – 46.

6. Kozin A. Steganography method using Hartley transform / A. Kozin, O. Papkovskaya, M. Kozina // Сучасні проблеми радіоелектроніки, телекомунікацій, комп'ютерної інженерії: матеріали XIII Міжнар. конф., 23.02–26.02.2016 р., Львів, Славське, Україна / Нац. ун-т "Львів. політехніка". – Л. : Вид-во Львів. політехніки, 2016. – С. 473-475.

7. Кобозева, А.А. Нечувствительность стеганосообщения к сжатию и формальные достаточные условия ее обеспечения / А.А. Кобозева, М.А. Мельник // Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка. – 2012. – Вип. 38. – С. 193–203.

8. Кобозева, А.А. Анализ чувствительности сингулярных векторов матрицы изображения как основа стеганоалгоритма, устойчивого к сжатию / А.А. Кобозева, М.А. Мельник // Захист інформації.– 2013. – Том 15, №2. – С. 88–96.

9. Мельник, М.А. Стеганоалгоритм, устойчивый к сжатию / М.А. Мельник – Інформаційна безпека. – 2012. - №2(8). – С. 99-106.

10. Кобозева, А.А. Стеганографический метод, обеспечивающий проверку целостности и аутентичности передаваемых данных / А.А. Кобозева, М.А. Козина // Проблемы региональной энергетики. Электронный журнал Академии наук Республики Молдова. – 2014. - №3(26). – С. 93-106.

11. Kozina, M.O. Steganography method of embedding information with singular value decomposition / M.O. Kozina, S.M., Njike Amougou / Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні - 2016. - №2.

12. Kobozeva, A.A. and Kozina, M.A. (2013). The steganographic method with a two-stage decoding which provids authentification the container. Informatics and Mathematical Methods in Simulation, 3(2), 169-178.

Надійшла: 23.04.2018 Рецензент: д.т.н. Шелест М.Є.