DOI 10.15276/imms.v12.no1-2.104
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 1-2, pp. 104-113

СТЕГАНОАНАЛІТИЧНИЙ АЛГОРИТМ, ЗАСНОВАНИЙ НА ДОСЛІДЖЕННІ СИНГУЛЯРНОГО РОЗКЛАДУ БЛОКІВ МАТРИЦІ ЦИФРОВОГО ЗОБРАЖЕННЯ

К.О. Трифонова, С.М. Сокальський

Національний університет «Одеська політехніка»,
1, пр. Шевченка, Одеса, 65044, Україна; e-mail: katikkatik@gmail.com

Одною з найпоширеніших технологій для забезпечення захисту будь-яких цифрових даних при передачі по відкритих каналах зв'язку, на поданий час, вважаються стеганографічні методи. Застосування розв'язку задачі захисту цифрових даних за допомогою стеганографічних методів, використовується не лише державними службами, але й терористичними організаціями. У зв'язку з цим, необхідність дослідження, розробки та постійного підвищення ефективності стеганоаналітичних методів, стає надзвичайно актуальним. В роботі запропоновано стеганоаналітичний алгоритм, заснований на дослідженні сингулярного розкладу блоків матриці цифрового зображення. Головною метою поданої роботи є підвищення ефективності стеганоаналізу цифрового зображення, у відсутності контейнеру, шляхом розробки нового стеганоаналітичного алгоритму, заснованого на дослідженні сингулярного розкладу блоків матриці цифрового зображення. В результаті детального дослідження стеганографічного алгоритму, що використовує сингулярний розклад блоків матриці цифрового зображення, встановлені статистичні характеристики сингулярних чисел блоків матриці зображення. На основі визначених характеристик, в роботі представлені основні кроки стеганоаналітичного алгоритму. В якості критерію для оцінки ефективності розробленого стеганоаналітичного алгоритму, використана ймовірність детектування додаткової інформації. Розглянуто помилки першого та другого роду. Для порівняння результатів роботи, розробленого стеганоаналітичного алгоритму з існуючими алгоритмами у відкритому доступі, обрані наступні застосування: XSteg; StegSpy. Для автоматизованого розв'язку стеганоаналітичної задачі для цифрового зображення реалізовано програмний продукт «StegoAnalysis».

Ключові слова: захист інформації, стеганоаналіз, цифрове зображення, сингулярні числа, сингулярні вектори.

Вступ

Задача реалізації захисту особистих та секретних даних від незаконного доступу, займає провідну позицію, як для кожної особистості окремо, так і для держави в цілому. Найбільш поширеною технологію для забезпечення захисту даних при передачі даних по відкритих каналах зв'язку є стеганографічні методи [1-5].

Для розв'язку задач захисту даних, стеганографія знаходить своє застосування не лише секретними службами, але й терористичними організаціями. У зв'язку з цим, задача розробки стеганоаналітичних методів, стає важливішою рік від року.

Методи виявлення секретного повідомлення в контейнері активно розроблюються [6]. В залежності від встановленого критерію, визначають різні способи класифікації існуючих стеганоаналітичних методів для цифрових зображень, представлених на рисунку 1 [7].

В залежності від наявної інформації у стеганоаналітика виділяють наступні групи стеганоаналітичних методів.

Спрямований. В поданому випадку передбачається, що доступна вся інформація про стеганографічний алгоритм. Невідомою виявляється інформація про стеганографічний ключ.

Універсальний. В поданому випадку жодної інформації про алгоритм вбудовування секретного повідомлення немає. Аналітик виконує роботу з дослідження та виявлення не характерних особливостей цифрових зображень.

В залежності від атаки розрізняють наступні групи стеганоаналітичних методів.

Статичний. Головним завданням поданих методів є розрізнення заповнених та порожніх контейнерів, встановлення методу занурення додаткової інформації.

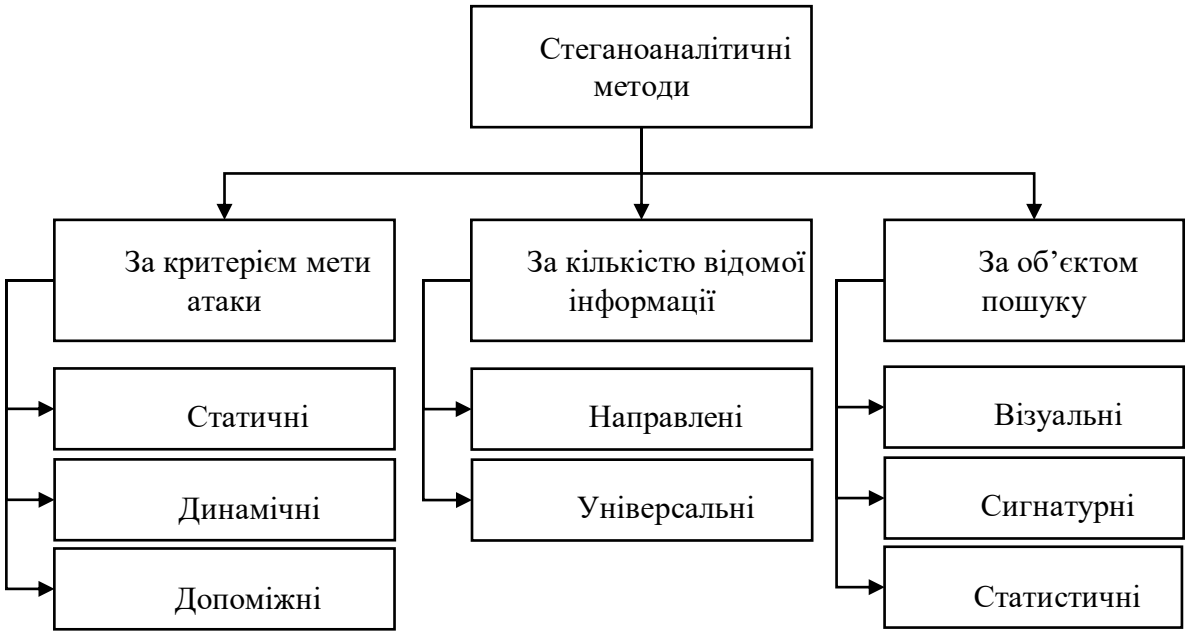


Рис. 1. Класифікація стеганоаналітичних методів

Динамічний. Головним завданням методів даної групи є визначення розміру вбудованого секретного повідомлення, його місце розташування, певні параметри алгоритму вбудовування, а також, в деяких випадках, навіть декодування приховуваного повідомлення.

Допоміжний. Головним завданням для даних методів є побудова різноманітних атак з метою активізації роботи стеганоканалу.

Стеганоаналітичні методи в залежності від предмета пошуку підрозділяють на наступні групи.

Візуальні. Методи, що відносяться до поданої групи, засновані на можливості людського зору встановлювати особливості цифрового зображення. При поданому аналізі відбувається дослідження графічного представлення контейнеру. Автоматизація такого типу методів, поки що є надзвичайно складним завданням, оскільки базується на розвитку методів комп'ютерного бачення та методів, що встановлюють характеристики справжності цифрових зображень.

Сигнатурні. Методи, що відносяться до поданої групи, засновані на дослідженні характерних особливостей формату зберігання цифрових зображень. Тобто пошук секретного повідомлення виконується в службових полях та полях даних. Методи сигнатурного допомагають виявити інформацію, яка була внесена у кінець файлу цифрового зображення Приховування інформації в такому випадку забезпечується тим, що стандартні програми перегляду зображень доходячи до маркеру кінця зображення припиняють свою роботу, і інформація, що находиться після цього маркеру залишається прихованою.

Статистичні. Методи, що відносяться до поданої групи, є найбільш поширеними. Подані методи засновані на дослідженні різноманітних статистичних характеристик натуральних, справжніх цифрових зображень.

Найбільш поширені методи, інформація про які наявна у відкритому доступі, відносяться до трьох груп: візуальні, сигнатурні, статистичні. Методи з кожної групи мають як свої переваги, так і не позбавлені значних недоліків, все це вимагає виконання нових досліджень, для розробки нових алгоритмів стеганографічного аналізу.

Мета і задачі дослідження

Метою роботи є підвищення ефективності стеганоаналізу цифрового зображення, у відсутності контейнеру, шляхом розробки нового стеганоаналітичного алгоритму, заснованого на дослідженні сингулярного розкладу блоків матриці цифрового зображення.

Для досягнення поставленої мети необхідно розв'язати наступні задачі:

1. виконати аналіз предметної області – дослідити реалізацію методів стеганоаналізу цифрових зображень;
2. виконати дослідження стеганоалгоритму, що використовує сингулярний розклад блоків матриці контейнера;
3. розробити стеганоаналітичний алгоритм, заснований на дослідженні сингулярного розкладу блоків матриці цифрового зображення;
4. реалізувати програмний продукт для виконання стеганоаналізу цифрового зображення.

Основна частина

Основні кроки алгоритму вбудовування секретного повідомлення стеганографічного алгоритму, заснованого на дослідженні сингулярного розкладу блоків матриці цифрового зображення, наведені в [8].

Ефективність цього стеганоалгоритму оцінюється за трьома критеріями: візуальна оцінка якості; ступінь забезпечення надійності сприйняття сформованого стеганоповідомлення; ступінь забезпечення надійності сприйняття стеганоповідомлення після атаки стисненням з різними ступенями стиснення.

Перш за все була проведена візуальна оцінка якості зображення після стеганоперетворення. В результаті експерименту було отримано набір стеганоповідомлень, для яких експертом не було виявлено жодних артефактів. На рисунку 2 наведено приклад цифрового зображення та зображення отриманого в результаті стеганоперетворення.

а) порожній контейнер б) заповнений контейнер

Рис. 2. Демонстрація результату стеганоперетворення

Наступним кроком оцінки стеганоалгоритму була оцінка надійності сприйняття стеганоповідомлення після атак стисненням. Важливо відмітити, що ці атаки були проведені за допомогою невеликих коефіцієнтів стиснення, оскільки важливо, щоб стеганоповідомлення зберігало надійність сприйняття після атак, інакше організатори прихованого каналу зв'язку можуть виявити факт використання атак стисненням. Тому атаки були використані із різним коефіцієнтом стиснення Q в діапазоні 80-100.

Експеримент проводився наступним чином. В обране цифрове зображення за допомогою стеганоперетворення вбудовувалась додаткова інформація, після чого воно зберігалось у форматі без втрат та у форматі з втратами з різними коефіцієнтами стиснення. Надійність сприйняття оцінена чисельно за допомогою пікового співвідношення сигнал-шум PSNR. Прийнято вважати, що надійність сприйняття не порушена, якщо PSNR > 37 Db. В ході експерименту встановлено, що для отриманих стеганоповідомлень подана нерівність не була порушена.

Стеганоаналітичний алгоритм, заснований на дослідженні сингулярного розкладу блоків матриці цифрового зображення

Стеганоаналітичні алгоритми можна класифікувати по різним критеріям. Наприклад, залежно від кількості наданої інформації для стеганоаналіза, методи розділяють на універсальні та направлені. Для направлених методів потрібно надати інформацію про стеганографічний алгоритм, за допомогою якого виконувалось стеганоперетворення. А при моделюванні універсального метода інформація про стеганографічний алгоритм може використовуватись лише в режимі «чорного ящика». При використанні такого класу методів стеганоаналітик старається найти деякі ознаки, які характерні для пустого контейнера, які одночасно задовольняли вимоги репрезентативності та контекстної незалежності, та змінювались би при стеганоперетворенні. Універсальні методи менш точні ніж направлені, але мають більш широкий спектр використання. Стеганоаналітичний алгоритм, заснований на дослідженні сингулярного розкладу блоків матриці цифрового зображення, відноситься до групи направлених алгоритмів. Основною метою поданого стеганоаналітичного алгоритму є встановлення факту наявності секретного повідомлення в контейнері цифрового зображення, що було піддано стеганоперетворенню на основі сингулярного розкладу блоків матриці цифрового зображення.

Розглянемо цифрове зображення F. Для кольорового цифрового зображення необхідно виконувати дослідження для кожної кольорової складової окремо. Матриця F розбивається стандартним чином на непересічні блоки f, розміром 8×8. Для кожного блоку виконується побудова сингулярного розкладу.

У відповідності до алгоритму стеганоперетворення вбудовування додаткової інформації в кожний блок виконується у відповідності до наступних формул:

$$\overline{\sigma}_1 = roundn(\sigma_1, K) + 1/4 \cdot \sigma_2, \quad (1)$$

для випадку вбудовування одиниці та

$$\overline{\sigma}_1 = roundn(\sigma_1, K) + 3/4 \cdot \sigma_2, \quad (2)$$

для випадку вбудовування нуля.

Позначимо співвідношення між першим та другим сингулярним числом блоку f матриці цифрового зображення F:

$$T = \frac{\overline{\overline{\sigma}}_1 - roundn(\overline{\overline{\sigma}}_1, K)}{\overline{\overline{\sigma}}_2}. \quad (3)$$

На основі поданої відомої інформації, зрозуміло, що після виконання стеганоперетворення, для заповненого контейнеру цифрового зображення, співвідношення між першим та другим сингулярними числами повинно відповідати наступним формулам:

$$\frac{\overline{\overline{\sigma}}_1 - roundn(\overline{\overline{\sigma}}_1, K)}{\overline{\overline{\sigma}}_2} \approx 1/4, \quad (4)$$

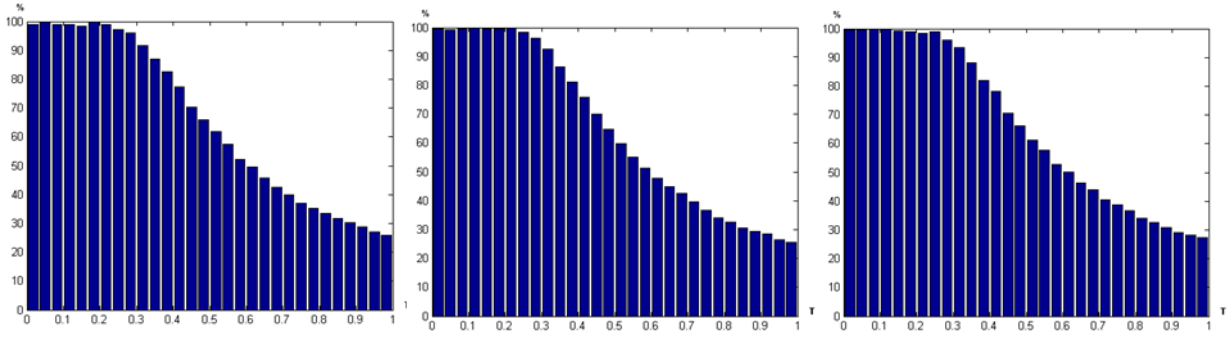
$$\frac{\overline{\overline{\sigma}}_1 - roundn(\overline{\overline{\sigma}}_1, K)}{\overline{\overline{\sigma}}_2} \approx 3/4. \quad (5)$$

Для підтвердження теоретичних висновків проведено обчислювальний

експеримент.

В експерименті задіяне 500 цифрових зображень різного розміру, що збережені в форматі без втрат та з втратами. Дослідження були виконані окремо для кожної кольорової складової: червоної, зеленої та синьої. Попередньо кожне цифрове зображення стандартним чином було розбито на блоки 8x8, для кожного блоку був побудований сингулярний розклад, та визначена величина T у відповідності до (3).

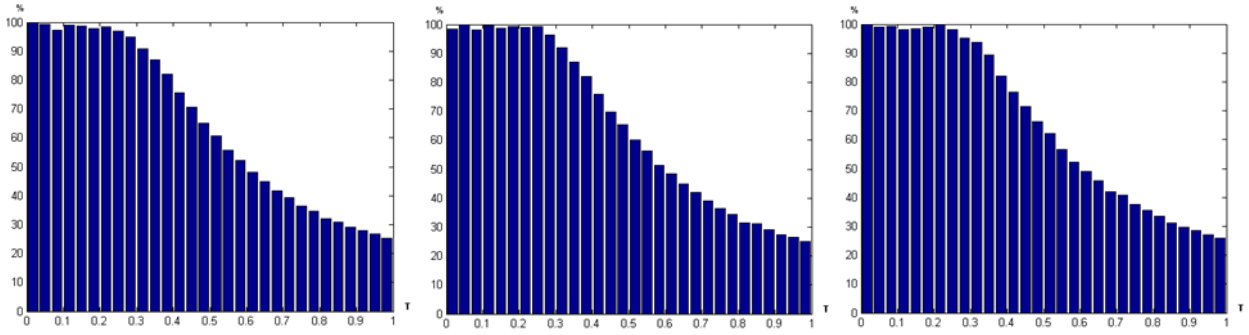
На основі отриманих даних побудовані для кожної кольорової складової усіх цифрових зображень збережених без втрат відповідні гістограми (рис. 3).



а) R б) G в) B

Рис.3. Гістограми значень T для порожніх контейнерів збережених без втрат

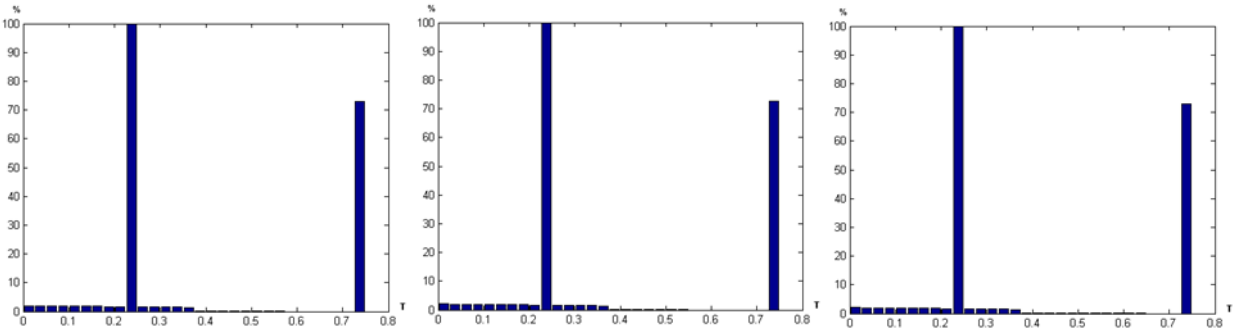
На основі отриманих даних побудовані для кожної кольорової складової усіх цифрових зображень збережених з втратами відповідні гістограми (рис. 4).



а) R б) G в) B

Рис.4. Гістограми значень T для порожніх контейнерів збережених з втратами

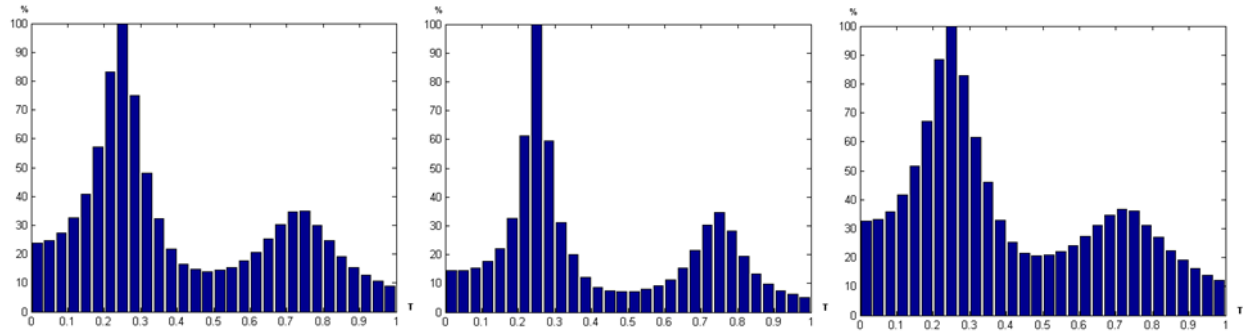
На основі отриманих даних побудовані для кожної кольорової складової усіх стеганоповідомлень збережених без втрат відповідні гістограми (рис. 5).



а) R б) G в) B

Рис.5. Гістограми значень T для заповнених контейнерів збережених без втрат

На основі отриманих даних побудовані для кожної кольорової складової усіх стеганоповідомлень збережених з втратами відповідні гістограми (рис. 6).



а) R б) G в) B

Рис.6. Гістограми значень T для заповнених контейнерів збережених з втратами

Основні кроки запропонованого стеганоаналітичного алгоритму наступні.

а) виконати розбиття матриці F стандартним чином на блоки f $8x8$;

б) виконати для кожного блоку f матриці F:

1) побудувати набір сингулярних чисел, в результаті $f = U\Sigma V^T$;

2) визначити величину $T(f) = \dfrac{\overline{\overline{\sigma_1}} - roundn(\overline{\overline{\sigma_1}}, K)}{\overline{\overline{\sigma_2}}}$;

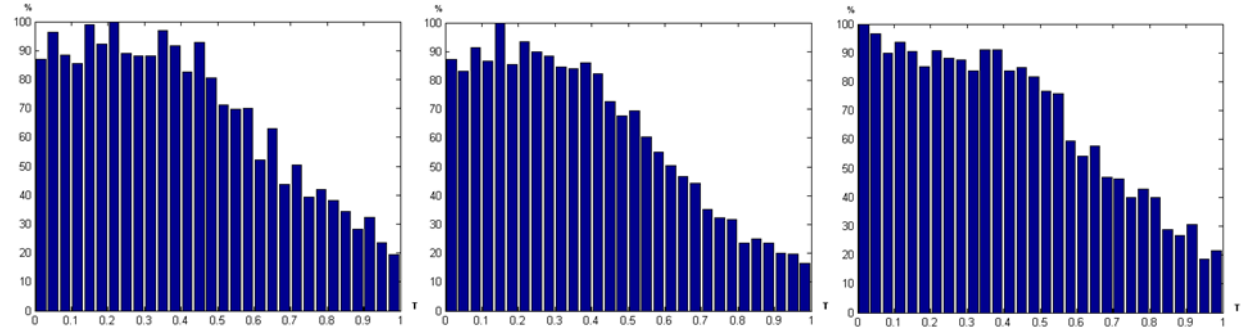
в) побудувати гістограму значень $T(f)$;

г) якщо $T(0{,}25) \geq T(0{,}5) \geq T(0{,}75)$, то F порожній контейнер,

якщо $T(0{,}25) > T(0{,}5) < T(0{,}75)$, то F заповнений контейнер.

Для демонстрації роботи, запропонованого стеганоаналітичного алгоритму, заснованого на дослідженні сингулярного розкладу блоків матриці цифрового зображення, розглянемо два цифрових зображення з рисунку 2.

Для цифрового зображення (рис. 2а) гістограми значень T представлені на рис. 7.



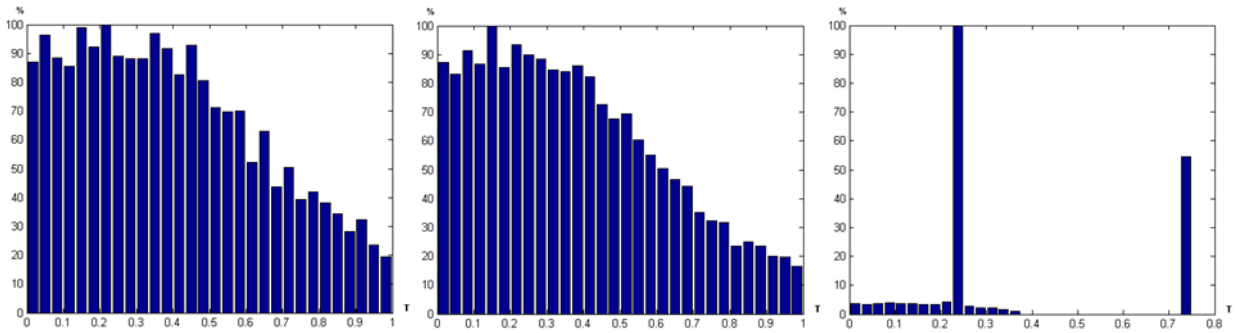
а) R б) G в) B

Рис.7. Гістограми значень T для порожнього контейнера збереженого без втрат

Для цифрового зображення (рис. 2б) гістограми значень T представлені на рис. 8.

Ефективність розробленого стеганоаналітичного алгоритму

В якості критерію для оцінки ефективності розробленого стеганоаналітичного алгоритму, заснованого на дослідженні сингулярного розкладу блоків матриці цифрового зображення, буде використана ймовірність детектування додаткової інформації. Розглянемо помилки першого та другого роду.



а) R б) G в) B

Рис.8. Гістограми значень T для заповненого контейнера збереженого без втрат

Помилка першого роду – випадок, коли стеганоаналітичний алгоритм визначає порожній контейнер як заповнений контейнер.

Помилка другого роду – випадок, коли стеганоаналітичний алгоритм визначає, що заповнений контейнер є порожнім.

Проведено обчислювальний експеримент. В експерименті задіяне 500 цифрових зображень різного розміру, що збережені в форматі без втрат та з втратами. В тестовому наборі були як порожні контейнери так і контейнери, що містили секретну інформацію. Кожний заповнений контейнер містив додаткову інформацію, вбудовану за допомогою стеганографічного алгоритму, заснованого на дослідженні сингулярного розкладу блоків матриці, в одну з кольорових складових. Для забезпечення надійності сприйняття порожнього або заповненого контейнеру, формат збереження з втратами обирався з невеликим ступенем стиснення. Вбудовування додаткової інформації, в матрицю обраної відповідної кольорової складової, відбувалось на 100%.

В результаті виконання експерименту встановлено, що помилки першого роду становили 1% та помилки другого роду 2%. Подані випадки представляють собою цифрові зображення невеликого розміру.

Для порівняння результатів роботи розробленого стеганоаналітичного алгоритму з існуючими алгоритмами у відкритому доступі, обрані наступні (рис. 9):

- C1 – стеганоаналітична програма XSteg [9];
- C2 – стеганоаналітична програма StegSpy [10];
- C3 – стеганоаналітична програма, заснований на дослідженні сингулярного розкладу блоків матриці цифрового зображення.

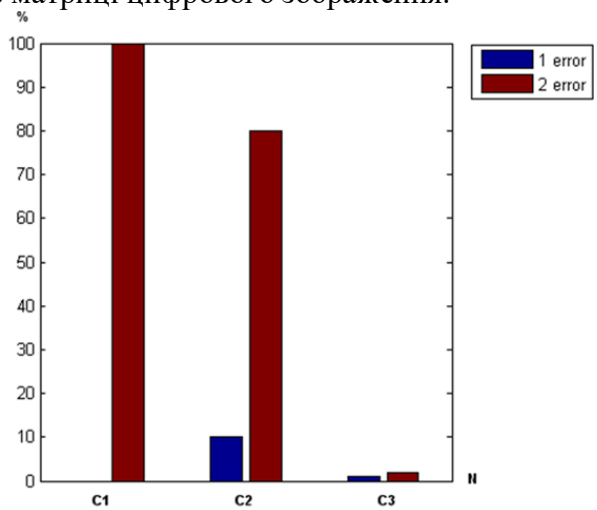


Рис. 9. Ефективність стеганоаналітичних методів

Для автоматизованого розв’язку стеганоаналітичної задачі для цифрового зображення реалізовано програмний продукт «StegoAnalysis», який складається з компонентів наступних програм [11-15]. Діаграма послідовності програмного продукту

«StegoAnalysis» зображена на рисунку 10.

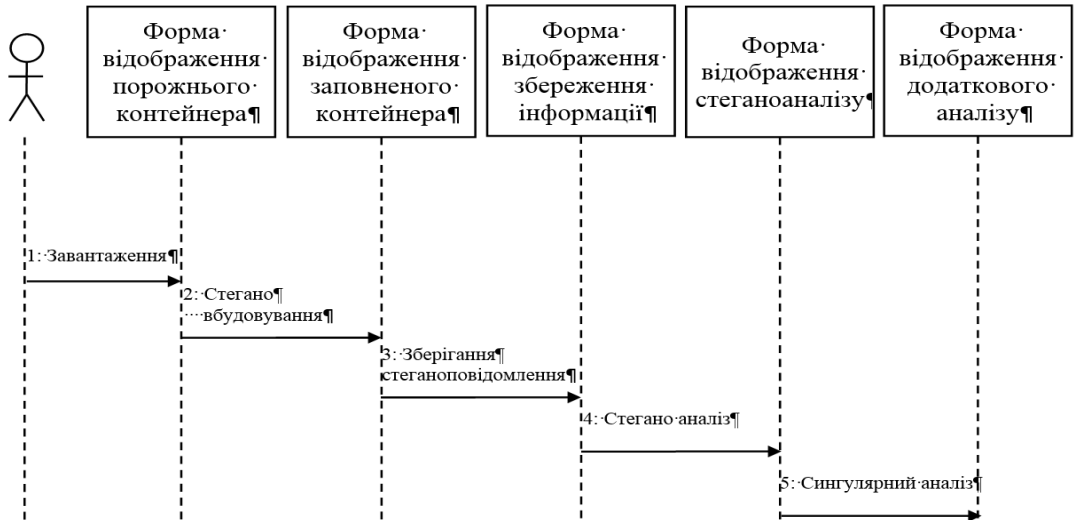


Рис. 10. Діаграма послідовності програмного продукту «StegoAnalysis»

Структура програмного продукту є модульною. Функціональна структура застосування включає в себе наступні модулі.

Модуль завантаження цифрового зображення: виконує завантаження контейнеру у різних форматах, як з втратами так і без.

Модуль стеганографічного перетворення: для виконання дослідження, реалізує стеганографічний алгоритм, заснований на дослідженні сингулярного розкладу блоків матриці цифрового зображення.

Модуль збереження стеганоповідомлення: реалізує можливість збереження заповненого контейнера у різних форматах, як з втратами так і без.

Модуль збереження секретного повідомлення: реалізує збереження генерованого секретного повідомлення.

Модуль стеганографічного аналізу: для виконання дослідження, реалізує стеганоаналітичний алгоритм, заснований на дослідженні сингулярного розкладу блоків матриці цифрового зображення.

Модуль сингулярного аналізу: додатково реалізує сингулярне дослідження для кожного блоку матриці цифрового зображення.

Інтерфейс програмного продукту представлено на рис.11.

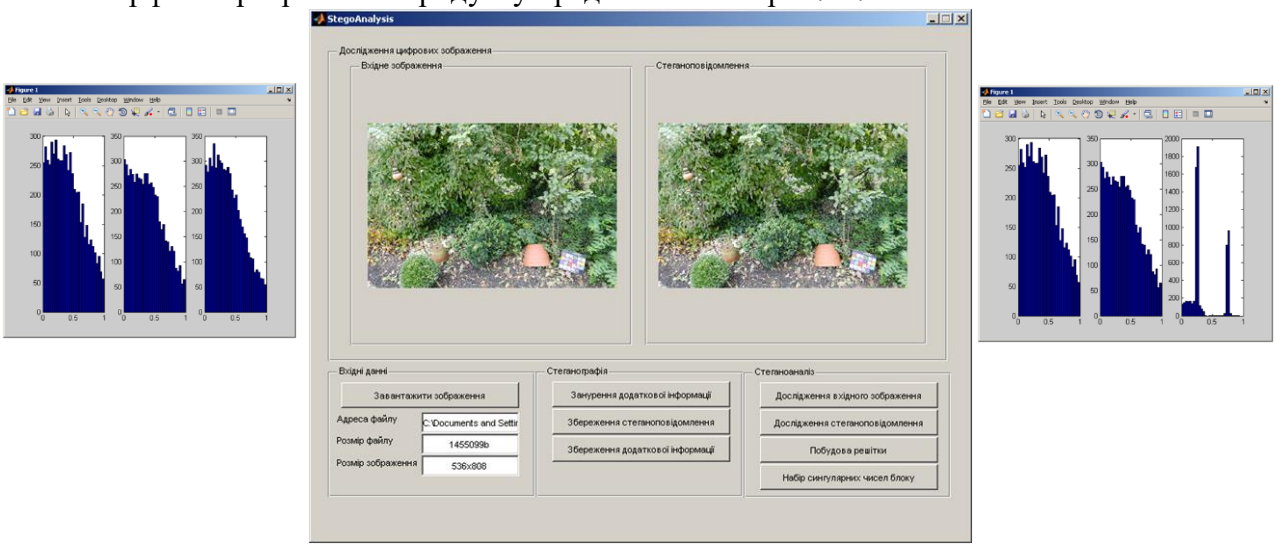


Рис. 11. Гістограми співвідношення першого та другого сингулярних чисел для кожної кольорової складової цифрового зображення

Висновки

В роботі представлені теоретичні основи стеганоаналітичного алгоритму, заснованому на дослідженні сингулярного розкладу блоків матриці цифрового зображення.

Детально виконано дослідження стеганоалгоритму, що використовує сингулярний розклад блоків матриці контейнера. Виявлено співвідношення між першим та другим сингулярними числами, що встановлюється в результаті вбудовування додаткової інформації. Проведено обчислювальний експеримент, що підтверджує теоретичні міркування.

На основі виявлених особливостей, розроблено стеганоаналітичний алгоритм, заснований на дослідженні сингулярного розкладу блоків матриці цифрового зображення.

Для оцінки ефективності розробленого стеганоаналітичного алгоритму підраховані помилки першого та другого роду.

Для автоматизованого розв'язку стеганоаналітичної задачі реалізовано програмний продукт «StegoAnalysis» для виконання стеганоаналізу цифрового зображення.

Список літератури

1. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. К.: МК-Пресс, 2006. 288 с.
2. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. К.: Юниор, 2003. 504 с.
3. Хорошко В.О., Яремчук Ю.Є., Карпінець В.В. Комп'ютерна стеганографія: навчальний посібник. Вінниця: ВНТУ, 2017. 155 с.
4. Аграновский А.В., Грибунин В.Г. Стеганография, цифровые водяные знаки и стегоанализ. М.: Вузовская книга, 2009. 220 с.
5. Грибунин В.Г., Туринцев И.В. Цифровая стеганография. М.: Солон-Пресс, 2009. 272 с.
6. Сокальський С.М., Трифонова К.О. Стеганоаналіз цифрових зображень. Актуальные научные исследования в современном мире. Сборник научных трудов. 2021. №5(73), Ч.2. С. 75–78.
7. Кошкина Н.В. Обзор и классификация методов стеганоанализа. Control Systems and Computers. Фундаментальные и прикладные проблемы Computer Science. 2015. № 3. С.3–12.
8. Козіна М.О., Папковська О.Б. Стеганоалгоритм, що використовує сингулярне розкладання матриці контейнера. Сучасний захист інформації. 2018. № 2(34). С.47–52.
9. XSteg. URL: https://launchpad.net/ubuntu/hoary/i386/xsteg/0.5-6
10. StegSpy. URL: http://www.spy-hunter.com/stegspy
11. Matlab. URL: https://www.mathworks.com/help/matlab/
12. Image Processing Toolbox. URL: https://www.mathworks.com/products/image.html
13. Документация IPT. URL: https://docs.exponenta.ru/images/index.html
14. IPT. URL: https://exponenta.ru/image-processing-toolbox
15. Matlab GUI. URL: https://www.mathworks.com/discovery/matlab-gui.html

STEGANOANALYTICAL ALGORITHM BASED ON THE STUDY OF THE SINGULAR DECOMPOSITION OF DIGITAL IMAGE MATRIX BLOCKS

K.O. Tryfonova, S.M. Sokalsky

National Odesa Polytechnic University
pr. Shevchenko, 1, Odesa, 65044, Ukraine; e-mail: katikkatik@gmail.com

Steganography methods are considered to be one of the most common technologies for the protection of any digital data when transmitted over open communication channels at a given time. The solution of the problem of digital data protection using steganography methods is used not only by government services, but also by terrorist organizations. Therefore, the need for research, development and continuous improvement of steganoanalytical methods is becoming extremely important. The steganoanalytical algorithm based on the study of the singular decomposition of digital image matrix blocks is proposed in the paper. The main purpose of this paper is to increase the efficiency of digital image steganoanalysis, in the absence of a container, by developing a new steganoanalytical algorithm based on the study of the singular decomposition of digital image matrix blocks. As a result of a detailed study of the steganography algorithm using the singular decomposition of digital image matrix blocks, the statistical characteristics of the singular values of image matrix blocks are established. Based on the defined characteristics, the paper presents the main steps of the steganoanalytical algorithm. As a criterion for assessing the effectiveness of the developed steganoanalytical algorithm, the probability of detecting additional information was used. Errors of the first and second type are considered. To compare the results of the developed steganoanalytical algorithm with existing algorithms in open access, the following applications are selected: XSteg; StegSpy. The software product "StegoAnalysis" has been implemented for the automated solution of the steganoanalytical problem for digital image.

Keywords: information security, steganoanalysis, digital image, singular values, singular vectors