УДК 004.056.5

Гончаров М.О., аспірант,
Малахов С. В., к.т.н., доцент,
Харківський національний університет імені В. Н. Каразіна

СПІРАЛЬНІ РОЗГОРТКИ БЛОКІВ ВИХІДНИХ ДАНИХ ЯК СПОСІБ ЗАХИСТУ СТЕГАНОГРАФІЧНОГО КОНТЕНТУ

Дана робота є продовженням циклу досліджень, присвячених відпрацюванню процедур обробки даних у рамках реалізації складових етапів малоресурсного стеганоалгоритму [1-2].

Як зазначалося у низці попередніх робіт [3-6], порядок вибірки (зчитування, розгортки або сканування) елементів вихідного масиву даних, є однією з найважливіших процедур у рамках реалізації принципу кодування довжин серій [7].

Згідно досліджуваної концепції алгоритму [2] стегановставки, застосування різних модифікацій методу кодування довжин серій, забезпечує вирішення відразу кількох завдань [2-6]: – оперативна оцінка статистичних характеристик вихідних масивів даних; – скорочення загального часу циклу стегановставки; – підтримка умов статистичного диспаритету даних у системі «контент–контейнер»; – створення стартових умов для подальшого мультиплексування діючих параметрів масиву серій, як механізму з протидії спробам неавторизованого вилучення контенту; – формування окремого рівня захисту від спроб несанкціонованого вилучення контенту.

Зважаючи на свою процедурну простоту, використання різних схем розгортки, забезпечує широку комбінаторність можливих станів формованих масивів серій, що суттєво посилює роль відповідного елемента в загальній структурі ключа екстрактора даних [5].

За принципом сканування масиву вихідних даних, розгортки можна умовно поділити на: – прості (лінійні); – складні (нелінійні); – двопрохідні; – випадкові; – комбіновані - тобто такі, що одночасно поєднують кілька схем (наприклад, двопрохідний варіант, у межах якого на кожному циклі, реалізується власна схема вибірки параметрів оброблюваного масиву) [3-4,6].

Представлений матеріал відображає результати застосування кількох варіантів спіральної розгортки, в умовах атаки тестового контенту. Як свідчить моделювання, спіральна розгортка є одним простих механізмів підвищення стійкості до спроб несанкціонованого вилучення прихованих даних. Це досягається завдяки суттєвому ускладненню просторової логіки послідовного доступу блоків

зображення без знання діючих параметрів «спіралі». До таких параметрів належать: – напрямок руху розгортки; – початкова точка старту; – розмірність ОБ; – модифікації патернів сканування (наприклад, однопрохідна чи двопрохідна спіраль). Завдяки такому варіативному розмаїттю спіральна розгортка набуває додаткової стійкості до геометричних і фрагментаційних атак (обрізання тощо).

На рис. 1 наведено результати атаки (*спроб неавторизованого вилучення*) тестового контенту для різних схем спіральної розгортки опорних блоків (ОБ) вихідних зображень. Моделювання проводилося з використанням напівтонових [7] тестових зображень (рис.1(а-б)) за умови помилкового відновлення контенту з використанням схеми «По рядках» [6]. Отримані результати демонструють стійкість спіральних схем до спроб нелегітимної екстракції прихованої інформації в умовах використання різних точок старту руху сканування.

Як слід з рис.1, спіральна розгортка суттєво ускладнює атакуючому задачу відновлення контенту. Інакше кажучи, спроби неавторизованого відновлення даних без знання діючих параметрів «спіралі» [3-5], зумовлюють значну фрагментацію відновлюваного масиву серій ОБ.

Результатом таких спроб, є лише фрагментовані, зображення (див. рис.1). Крім того, корисні наслідки від використання спіральної схеми розгортки виявляються при геометричних спотвореннях і частковій втраті зображення. Так, у разі обрізання певної частини зображення, втрачається лише частина умовних витків спіралі, а не цілі лінійні сегменти даних, як це відбувається при класичних растрових чи зигзагоподібних розгортках [4,6]. Це суттєво ускладнює відновлення повної прихованої інформації, навіть при помірних геометричних спотвореннях чи частковій втраті контенту.

Наприклад, якщо прихований контент розміщується всередині зображення саме за спіральною схемою, то дані розподіляються нелінійно по всій площі носія (контейнеру), а не концентруються в окремих рядках, стовпцях чи блоках.

Завдяки цьому спіральна схема стає значно стійкішою до типових маніпуляцій з зображеннями, таких як: обрізання країв, компресія з втратами, масштабування та незначні повороти. Навіть при втраті частки площі зображення, значна частина витків спіралі зберігається, дозволяючи авторизованому користувачу [5] вилучати, принаймні, частину повідомлення або повністю відновити його за умови використання додаткових механізмів корекції помилок.

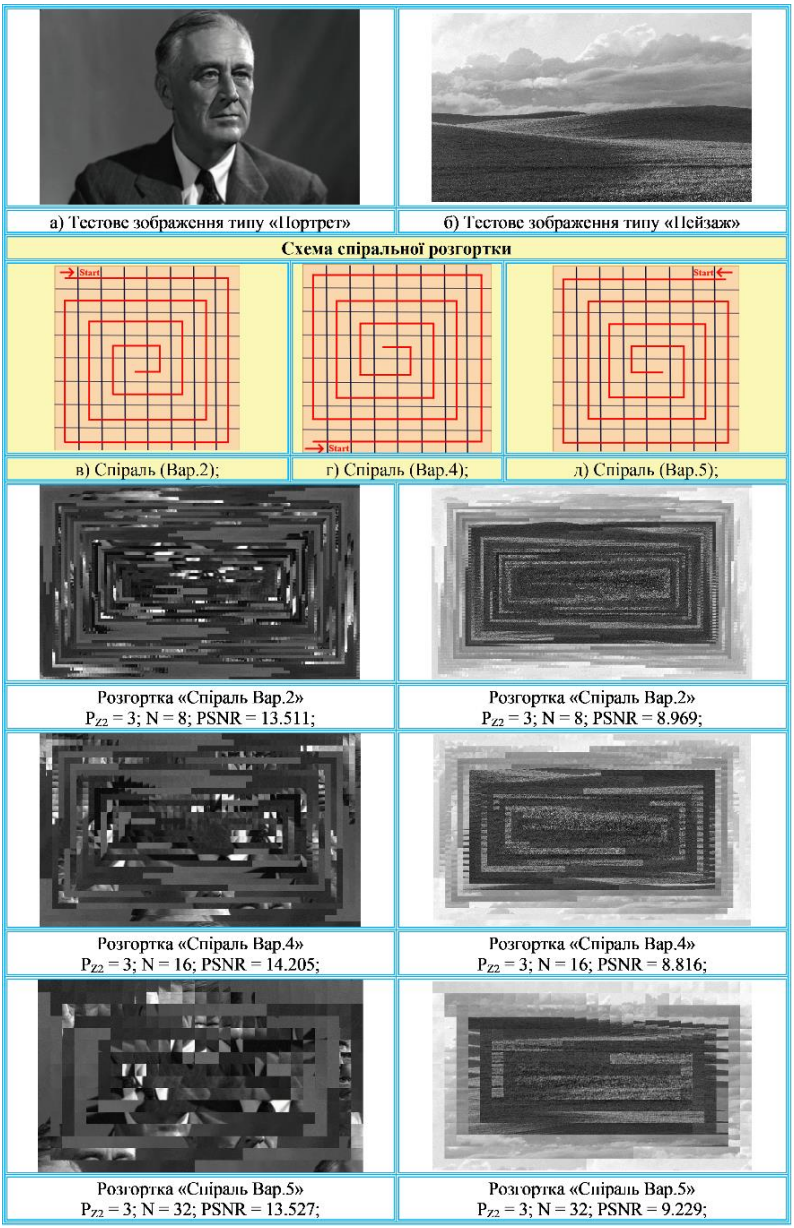

Рисунок 1 – Результати атаки тестового контенту для різних схем «спіралі» та розмірностей ОБ (*хибне відновлення за схемою «По рядках»*)

Висновок. Проведене моделювання підтвердило, що застосування спіральної розгортки не лише підвищує захист до спроб підбору діючої послідовності кодування контенту, але й забезпечує помітно кращу робастність до типових маніпуляцій з зображеннями, порівнянно з простими схемами [3-4]. Це значно посилює можливості алгоритму малоресурсної стегановставки, роблячи спіральний принцип розгорток, надійним й обчислювально ефективним інструментом з протидії спробам неавторизованого вилучення даних.

Список використаних джерел

1. Honcharov M., Liesnaia Y., Malakhov S. Investigation of the properties of the prototype of a hybrid steganographic algorithm // *Computer Science and Cybersecurity*. 2021. № 2. С. 45-56. URL: https://doi.org/10.26565/2519-2310-2021-2-05

2. Honcharov M. O., Nariezhnii O. P., Malakhov S. V. Analysis of prerequisites for ensuring resource consensus when performing steganographic data insertion procedures. *Modern Information Security*. 2025. № 3. С. 37–47. URL: https://doi.org/10.31673/2409-7292.2025.030518

3. Гончаров М. О., Малахов С. В., Жілєнков Д. В. Дослідження складності та властивостей різних схем розгортки вихідних даних стеганоконтента, в умовах зміни сценаріїв атак. *Сучасний захист інформації.* 2025. № 4. С. 44–58. DOI: 10.31673/2409-7292.2025.041205

4. Гончаров М., Малахов С. Дослідження способів розгортки вихідних блоків зображення-стеганоконтенту як механізму протидії від несанкціонованої екстракції даних. *Science and Technology Today*. 2023. № 4 (18). С. 293–308. URL: https://perspectives.pp.ua/index.php/nts/article/view/4445

5. Honcharov M., Malakhov S. Modeling attempts of unauthorized extraction of steganocontent under different combinations of data key-extractor. *Collection of Scientific Papers «ΛΟΓΟΣ»* (Paris, France, March 1, 2024). 2024. P. 234–245. URL: https://doi.org/10.36074/logos-01.03.2024.053

6. Лєсная Ю., Гончаров М., Семенов А., Малахов С. Моделювання розгортки серій опорних блоків зображення, як інструменту з протидії спробам несанкціонованої екстракції стеганоконтенту. *Collection of Scientific Papers «ΛΟΓΟΣ»* (Zurich, Switzerland, March 31, 2023). 2023. С. 109–115. URL: https://doi.org/10.36074/logos-31.03.2023.33

7. Pratt W. K. Digital Image Processing. New York : John Wiley & Sons, 1978. 750 p.