ABSCHNITT XVII. INFORMATIONSTECHNOLOGIEN UND –SYSTEME

DOI 10.36074/logos-31.03.2023.33

МОДЕЛЮВАННЯ РОЗГОРТКИ СЕРІЙ ОПОРНИХ БЛОКІВ ЗОБРАЖЕННЯ, ЯК ІНСТРУМЕНТУ З ПРОТИДІЇ СПРОБАМ НЕСАНКЦІОНОВАНОЇ ЕКСТРАКЦІЇ СТЕГАНОКОНТЕНТУ

НАУКОВО-ДОСЛІДНА ГРУПА:

Лєсная Юлія Євгеніївна
студентка факультету комп'ютерних наук (магістратура)
Харківський національний університет імені В.Н. Каразіна

ORCID ID: 0000-0002-9790-7260 **Гончаров Микита Олександрович**
магістр факультету комп'ютерних наук
Харківський національний університет імені В.Н. Каразіна

Семенов Артем Сергійович
студент факультету радіоелектроніки, комп'ютерних систем та інфокомунікацій (бакалаврат)
Національний аерокосмічний університет ім. М.Є. Жуковського, "ХАІ"

ORCID ID: 0000-0001-8826-1616 **Малахов Сергій Віталійович**
канд. техн. наук, ст. науковий співробітник, доцент кафедри
Харківський національний університет імені В.Н. Каразіна

УКРАЇНА

Вступ. Представлені результати моделювання різних способів сканування (*надалі розгортки*) опорних блоків (ОБ) [1-3] зображення-контенту при імітації умовної атаки стеганоконтенту в припущенні, що атакуючої стороні вдалося підібрати поточні параметри обробки контенту [4], які реалізовані на двох основних рівнях захисту (*міжблоковому і внутріблоковому, рис. 2-4* [5]) дослідного стегоалгоритму. Дана робота є продовженням циклу досліджень, щодо уточнення можливостей протидії спробам нелегітимної екстракції даних, за рахунок розширення варіативності способів розгортки серій ОБ [4,6-7].

Тестове зображення і схеми розгортки, що були досліджені в межах реалізованого імітаційного моделювання, представлені на рис.1. **Основна частина.** Слід мати на увазі, що діючий спосіб організації розгортки серій ОБ [3] визначається відповідним елементом в структурі ключа екстрактора даних (*елемент №2 в табл.1* [6]). Характерні результати атаки (*спроб несанкціонованого вилучення*) тестового зображення-контенту при реалізації деяких схем розгортки представлено в роботах [4,6]. В роботі [7] наведені результати спроб неавторизованої екстракції контенту при реалізації режиму двопрохідної розгортки (*тобто черезблокової вибірки*) серій ОБ для тестового зображення типу «портрет» *(див. рис.1, зразок (m))*.

На рис.2-3 представлені результати, що характеризують *загальну кількість* ОБ та *середню довжину* серій для схем розгорток, що наведені на

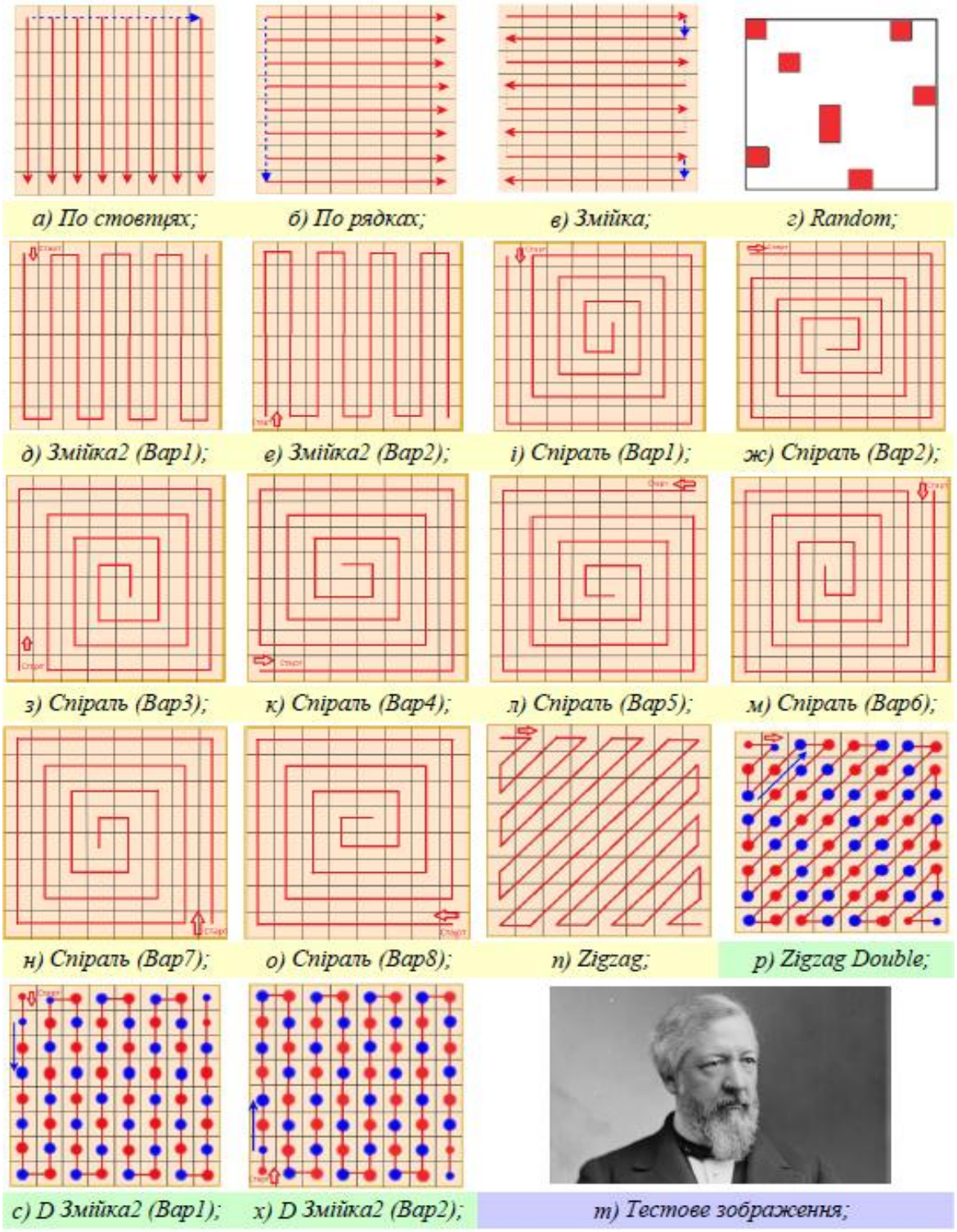


Рис. 1. **Досліджувані способи розгортки серій ОБ** *(а-х)* **та тестове зображення** *(т)*

рис.1. При цьому, імітаційне моделювання атаки тестового контенту проводилося для трьох розмірностей блоків зображення: 4×4, 8×8 та 16×16 елементів.

Двопрохідна (*черезблокова*) модифікація розгорток *(вар. (р-х) на рис.1)* при першому скані вихідного масиву контенту, передбачає послідовну вибірку всіх непарних блоків *(червоні маркери в зразках (р-х) на рис.1)*, а при повторному проході/скані, всіх парних блоків контенту *(сині маркери).*

Слід зазначити, що всі способи розгортки (рис.1) не є обчислювально складними, але дозволяють значно ускладнити «роботу» атакуючого, посилюючи загальний захисний потенціал алгоритму [4,6].

З рис.2 видно, що збільшення розмірності блоків призводить до різкого зменшення *(див. порівняння синій та червоній гістограм)* кількості серій ОБ зображення [2], причому для всіх розглянутих способів розгорток (рис.1). При цьому використання блоків великих розмірностей *(червона гістограма на рис.2)* практично усуває різницю в кількості серій ОБ для різних способів розгортки. Іншими словами, показник, що характеризує кількість серій, які формуються, значною мірою залежить від діючого параметра/способу розгортки і зменшується зі збільшенням розмірності ОБ.

Застосування двопрохідної розгортки *(рис.1, Вар.(р-х))*, за показником сформованих серій ОБ, порівняно з використанням режиму випадкової розгортки *(Вар.(г) на рис.1)*, дає дуже близькі результати, причому для всіх розглянутих розмірностей блоків. При цьому візуальна фрагментація *(тобто руйнування структури)* атакованого контенту для зазначених вище випадків значно відрізняється *(див. рис. 4)*. Іншими словами, при загальній схожості вихідного набору серій, що формується, випадковий режим розгортки *(Random)* забезпечує більшу взаємну фрагментацію ОБ.

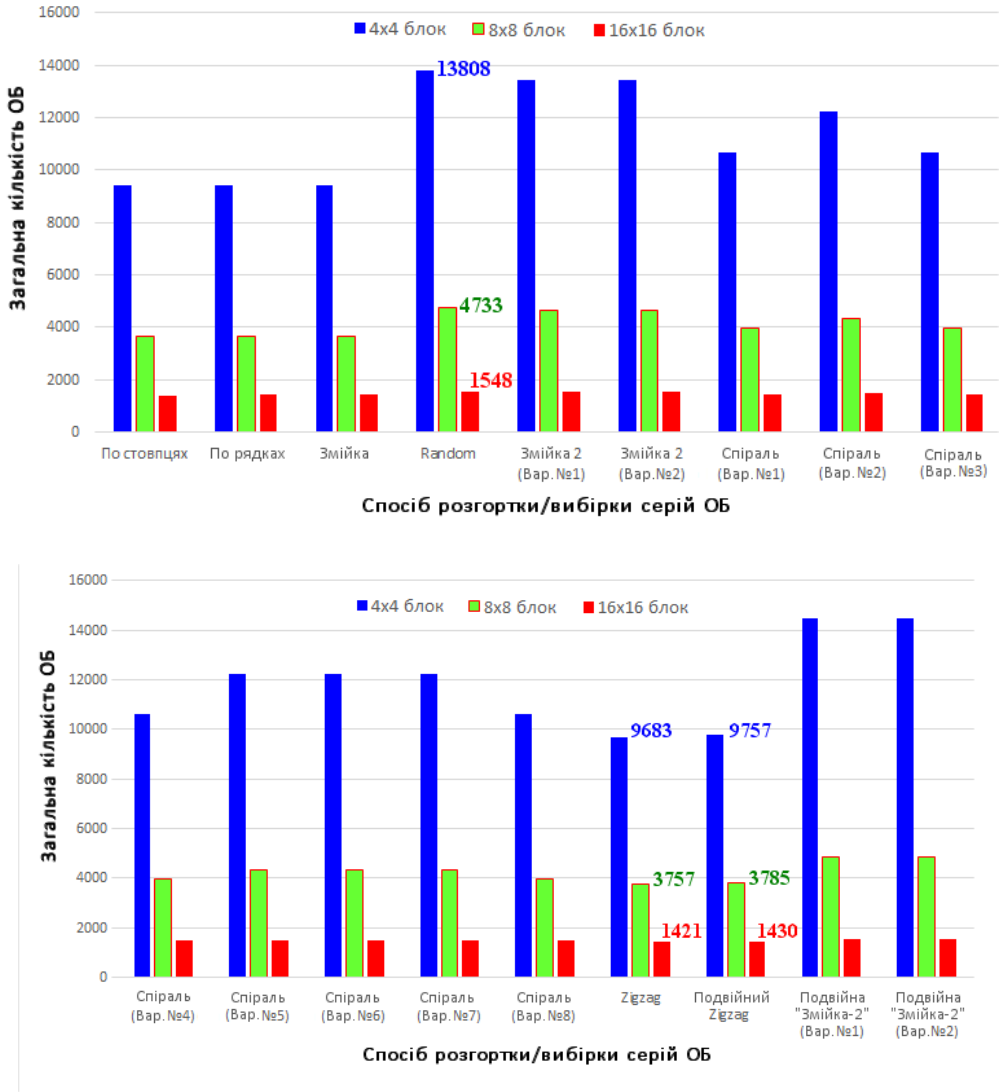


Рис. 2. **Кількість ОБ для різних способів розгортки та розмірностей ОБ** *(тестове зображення типу портрет, зразок (т) на рис.1)*

Проте все має власну ціну і за посилення ефекту візуальної фрагментації вихідного контенту доводиться чимось «платити». Так, використання «складних» способів і режимів розгортки *(у даному випадку двопрохідної та/або рандомної)* помітно збільшує загальну кількість серій, що є небажаним з погляду зменшення загальної обчислювальної складності всього алгоритму. Така тенденція призводить до збільшення загальної кількості блоків, що вимагають проведення кодування з перетворенням [8], безпосередньо перед реалізацією процедур мультиплексування параметра середньої яскравості ОБ на 2-му рівні захисту (*крок №6 на рис.1 в* [4]) дослідного алгоритму [1].

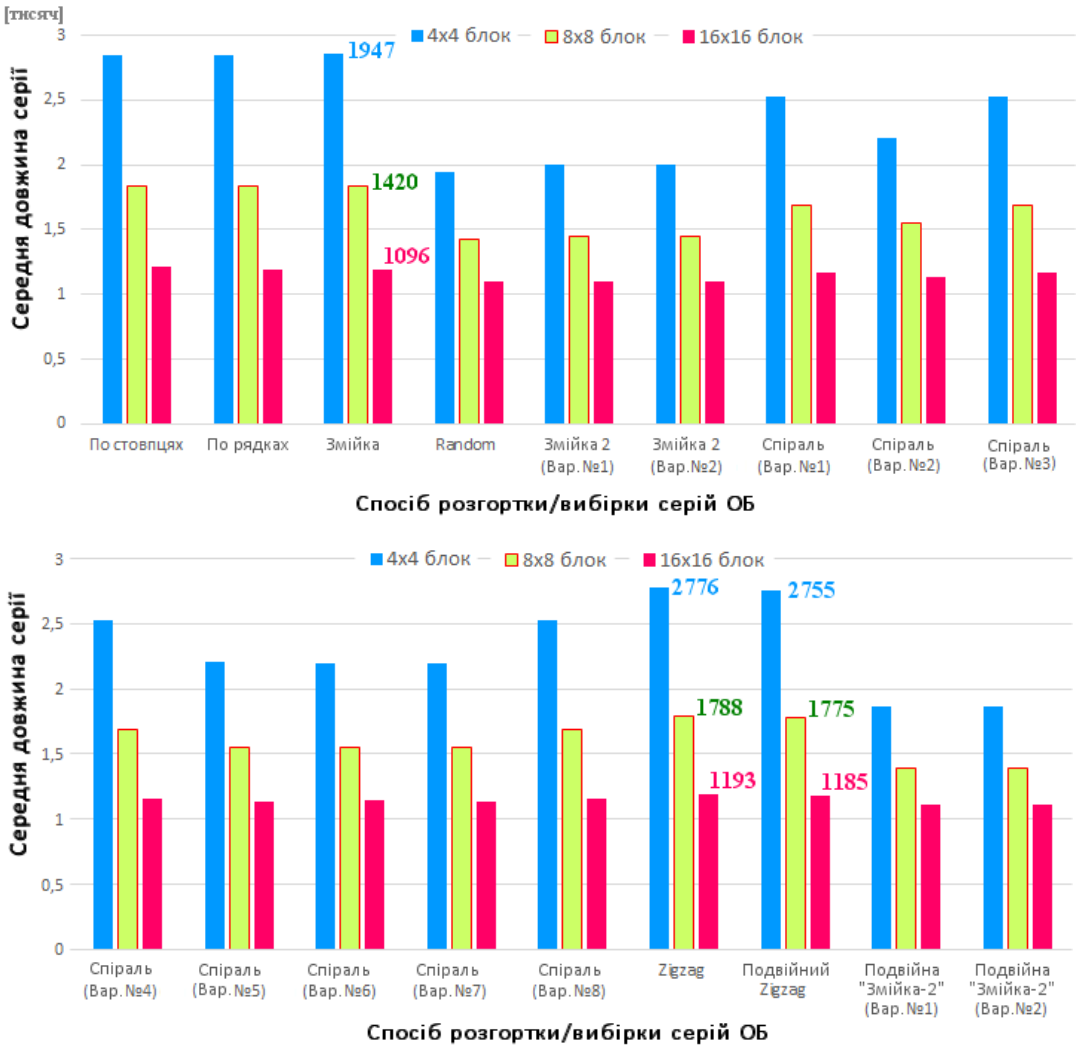
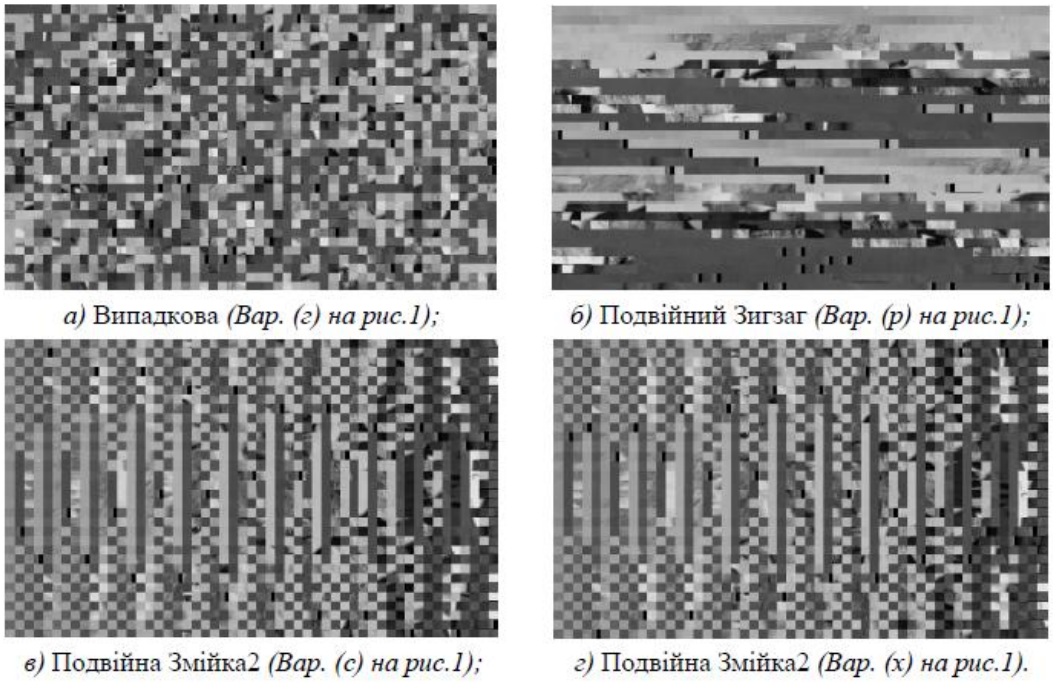


Рис. 3. **Середня довжина серії для різних способів розгортки та розмірностей ОБ**

Основною метою проведеного моделювання була, демонстрація важливості знаходження потрібного компромісу між: 1 – складністю реалізації того чи іншого способу розгортки і, відповідно, її можливостей щодо протидії спробам ідентифікації та неавторизованої екстракції контенту; 2 – зменшенням загальної кількості серій, що формуються, як запоруки процесу зменшення обчислювальної складності всього алгоритму [1-2].

Як слід з рис.2, з точки зору дотримання подібного балансу, найкращим варіантом є використання розгортки типу *«Зигзаг» (рис.1, Вар.(н-р))*, яка забезпечує одночасне та пропорційне сканування масиву вихідного контенту, як

по вертикалі, так і по горизонталі. Така розгортка відчутно ускладнює ідентифікацію отриманої сцени *(рис.2 (a-b) в [6])*, причому: 1 - без непрямої вказівки на використану схему сканування; 2 - небажаного збільшення обчислювальної складності на 2-му рівні захисту *(кроки 5-6 на рис.1 в [4])*, що властиво для режиму рандомної розгортки *(рис.2 (ж-з) в роботі [6])*.



а) Випадкова *(Вар. (г) на рис.1);* *б)* Подвійний Зигзаг *(Вар. (р) на рис.1);*

в) Подвійна Змійка2 *(Вар. (с) на рис.1);* *г)* Подвійна Змійка2 *(Вар. (х) на рис.1).*

Рис. 4. **Результати атаки тестового контенту для різних способів розгортки серій с розмірністю ОБ 16×16 ел.**
(при умові помилкового відновлення [4] контенту по Рядках, Вар. (б) на рис.1)

Використання режиму подвійного сканування в діапазоні розмірностей ОБ від 4×4 до 8×8 ел., помітно збільшує кількість серій, які формуються, що добре видно при порівнянні гістограм *«Змійка 2»* і *«Подвійна Змійка 2»* на рис. 2, та порівняні зразків *(в)* із *(д)*, та *(г)* із *(е),* на рис.1 в роботі [7].

Аналіз гістограми на рис. 3 дозволяє виділити деякі способи розгортки, що забезпечують формування серій ОБ з найбільшою довжиною. При цьому слід враховувати дві важливі обставини: 1 – тип контенту, що обробляється *(з точки зору його статистичних властивостей [8])*; 2 – ступінь складності зворотної компіляції вихідного контенту під час спроб роботи атакуючого зі «зламаним» масивом даних [4,6].

Природно, що для різних типів зображень [8], гістограми на рис.2-3 мають різні характеристики, проте в межах даної роботі представлені результати моделювання лише для напівтонових зображень типу «портрет», характерний зразок якого представлений на рис.1*(т).* А ось, з точки зору складності зворотної компіляції вихідного контенту, з усього тестового набору розгорток (рис.1), насамперед слід виділити схему, яка реалізує принцип *«Зигзаг»* (*рис.1 (Вар. (п) та (р))*. Так, при всій схожості одержуваних результатів у порівнянні з розгортками *«По стовбцях»*, *«По рядках»* і *«Змійка»*, саме «*Зигзаг*» забезпечує найбільшу візуальну фрагментацію контенту та позбавляє атакуючого непрямих підказок у частині реалізованого способу розгортки.

Характерні результати атаки контенту під час реалізації «простих» схем розгортки (*Вар. (а)-(в), на рис.1*), представлені на рис.4 у роботі [5]. Прикладом

непрямих підказок, щодо реалізованого способу розгортки, служать зразки атакованого контенту, котрі представлені на рис. 3*(в-е)* у роботі [4], та на рис. 4 в роботі [5]. Вказані зразки зображень, зважаючи на характерну структуру візуальних артефактів, дають атакуючій стороні можливість локалізації вектора можливих пошуків, стосовно реалізованої схеми розгортки *(рядки, стовпці або спіраль тощо, рис.4, [5])*. Знов-таки, варіант рандомної розгортки *(рис. 3(ж-з) в роботі [4])* не розглядається як пріоритетний (з точки зору ступеня візуальної фрагментації контенту), через зменшення середньої довжини серій, що формуються, у найбільш збалансованому, з практичного боку, діапазоні розмірностей блоків (*тобто, близько 8×8 ел., див. рис. 2*).

Узагальнюючи все вищесказане, можна констатувати, що розгортки котрі реалізують схему *«Зигзаг»*, найкращім чином поєднують в собі особливості структури що притаманні для зображень типу портрет, та забезпечують найкращі умови для максимального утруднення процедур зворотної компіляції вихідного контенту. Крім того, можливість реалізації різних схем *«Зигзагу» (наприклад, «старт» у різних точках та/або черезблочна розгортка)* додатково нарощує комбінаторику відповідного елементу в структурі ключа екстрактора даних (*рис. 1 в роботі [6]*). Таким чином, навіть у разі компрометації основних захисних механізмів *відразу* на двох рівнях мультиплексування [4-5] використання різних варіацій схеми розгортки типу *«Зигзаг»* дозволяє успішно протидіяти спробам нелегітимної екстракції контенту.

Висновки.

1. Проведене моделювання має демонстраційний характер та дозволяє візуалізувати наслідки використання різних схем розгортки серій ОБ контенту при умові компрометації відразу обох основних рівнів [4-5] захисту дослідного стегоалгоритму, де в якості тестових зображень виступала відповідна добірка напівтонових зображень типу «портрет».

2. Проведене моделювання демонструє, що вдалий підбір (*атака*) діючих параметрів обробки даних, відразу на двох основних рівнях захисту, не гарантує успішної зворотної компіляції вихідного контенту, що добре підтверджують відповідними зразками тестових зображень на рис. 4.

3. За результатами моделювання визначено, що реалізація різних варіацій схеми розгортки типу *«Зигзаг»*, має малу обчислювальну складність, проте не дає атакуючому простого рішення, стосовно спроб нелегітимної екстракції контенту (*див. рис.4(б) в роботі* [4] *та рис. 1(в),(д) в роботі* [7]).

4. При обробці зображень типу «портрет», схема розгортки, що реалізує принцип *«Зигзаг»*, в порівнянні з *іншими* типами розгорток, забезпечує найбільшу візуальну фрагментацію вихідного контенту та позбавляє атакуючого непрямих підказок щодо втіленої схеми розгортки.

Список використаних джерел:

[1] Гончаров, М., Лєсная, Ю., & Малахов, С. (2021). Дослідження властивостей прототипу гібридного стеганоалгоритму. Комп'ютерні науки та кібербезпека, (2), 45-56. Вилучено з URL: https://periodicals.karazin.ua/cscs/article/view/18183

[2] Гончаров О., Лєсная Ю., Погоріла К., Богданова Є., Малахов С. Дослідження параметру «серій опорних блоків», як елементу композитного ключа екстрактора даних стеганоалгоритму // Problems of science and practice, tasks and ways to solve them. Proceedings of the XX International Scientific and Practical Conference. Warsaw, Poland. 2022. Pp. 779-785. Вилучено з URL http://surl.li/fpatz

[3] Гончаров, Н., Лесная, Ю., & Малахов, С. (2022). Адаптация принципа кодирования длин серий для противодействия попыткам неавторизованной экстракции стеганоконтента. Grail of Science, (17), 241–247. https://doi.org/10.36074/grail-of-science.22.07.2022.042

[4] Лесная, Ю., Гончаров, Н., & Малахов, С. (2023). Способы развертки параметров серий опорных блоков изображений, как элемент составного ключа экстрактора данных стегоалгоритма. Grail of Science, (23), 254–258. https://doi.org/10.36074/grail-of-science.23.12.2022.37

[5] Лєсная, Ю., Гончаров, М., & Малахов, С. (2023). Результати моделювання спроб несанкціонованого вилучення стеганоконтенту для різних комбінацій атаки дослідного стегоалгоритму. Scientific Collection «InterConf», (141), 338-345. http://surl.li/foonl

[6] Лєсная, Ю., Гончаров, М., Азаров, С., & Малахов, С. (2023). Візуалізація спроб несанкціонованої екстракції стеганоконтенту при помилковому визначенні діючих способів розгортки серій. Grail of Science, (24), 335–340. https://doi.org/10.36074/grail-of-science.17.02.2023.061

[7] Лєсная, Ю., Гончаров, М., Малахов, С., & Мелкозьорова, О. (2023). Результати несанкціонованої екстракції стеганоконтенту при реалізації двохпрохідної розгортки серій вихідних блоків. *Collection of Scientific Papers «ΛΌГОΣ»*, (March 3, 2023; Bologna, Italy), 65–67. https://doi.org/10.36074/logos-03.03.2023.19

[8] Прэтт У. (1985). *Цифровая обработка изображений* (Д. С. Лебедева, пер. с англ.). т. 1,2. Москва: Мир.