УДК 004.056.55
DOI: 10.31673/2409-7292.2026.010115

Борисенко І.І.

ПРОБЛЕМА ВИБОРУ КОНТЕЙНЕРА ДЛЯ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ СТЕГО ДО ЗБУРНИХ ДІЙ

У епоху цифрових технологій захист мультимедійної інформації, веб сайтів, організація надійних способів передачі та зберігання даних, особливо конфіденційної інформації, стали важливими аспектами будь-якого бізнесу чи організації і активно розвиваються. В комплексних системах захисту інформації широке застосування знайшли стеганографічні методи, принцип роботи яких полягає в створенні прихованих каналів зв'язку у вже існуючих потоках даних в інформаційно-телекомунікаційних системах. Однією із найважливіших вимог є забезпечення стійкості стеганосистеми до атак стеганоаналізу. Статистичні методи стеганоаналізу намагаються виявити найменші зміни у статистичній поведінці файлу-контейнера, викликані стеганографічним перетворенням. Задача вибору стеганографічного контейнера шляхом знаходження в ньому елементів, найменш чутливих до збурень, які вносяться під час вбудовування повідомлення, дозволяє задовольнити деякі із вимог, що ставляться перед стеганосистемою при її побудові. Атаки проти вбудованого повідомлення не вимагають від зловмисника фундаментальних знань у галузі стеганоаналізу, не вимагають наявності спеціальних технічних засобів, що робить даний вид атак простим та розповсюдженим. Тому апріорна формальна оцінка збурень матриці контейнера при його стеганографічному перетворенні є важливою задачею і є метою даної роботи. В роботі запропоновано метод кількісної оцінки збурень контейнера під час його стеганографічного перетворення, який дозволяє побудову більш ефективних алгоритмів за рахунок мінімізації впливу вбудованого повідомлення на контейнер. Побудована функція, яка дозволяє виконати аналіз збурень, які виникають під час вбудовування повідомлень різними стеганографічними алгоритмами, що дає можливість порівнювати їх ефективність. Наведені результати обчислювального експерименту, які підтверджують ефективність запропонованого методу.

Ключові слова: вбудоване повідомлення, збурення контейнера, стеганографічне перетворення, стійкість стеганосистеми, ефективність стегометода.

Вступ та формулювання проблеми

З розвитком технологій захисту інформації також розвиваються і способи отримання несанкціонованого доступу до конфіденційної інформації, її зміни або знищення, тому завдання покращення методів прихованої передачі та зберіганні даних залишається актуальним і на сьогоднішній день.

Основною метою використання комп'ютерної стеганографії є приховування повідомлень в цифрових даних (ЦД), які, як правило, мають аналогову природу (мова, зображення, аудіо або відеозапис). Це ефективний засіб захисту інформації, який стає особливо актуальним у випадку, коли застосування криптографічних методів неможливо або обмежено. В якості повідомлення виступає будь-яка конфіденційна інформація (особисті та медичні дані, банківська та комерційна інформація і т.п.), яка повинна бути вбудована таким чином, щоб навіть сам факт її присутності у контейнері був таємним. ЦД, в які вбудовується повідомлення, носять узагальнену назву – контейнер, результатом такого вбудовування є стеганоконтейнер (стего) або стеганографічне повідомлення, яке відкрито пересилається одержувачу каналами загального користування

Зі зростанням кількості і складності стеганографічних методів та алгоритмів приховування повідомлень зростає також і кількість методів стеганоаналізу, які переслідують мету виявлення стеганографічних вкладень.

Програмні інструменти приховування інформації такі як Steganos, Outguess, Jsteg, Jphs, S-Tools та інші прості в використанні і здатні створити стеганографічний канал з великою пропускною здатністю. Ці інструменти, як правило, використовують метод найменшого значущого біта (LSB) та його модифікації, але стеганоконтейнери, які створені за допомогою LSB, успішно виявляються методами стеганоаналізу. Цей факт призвів до появи цілого ряду робіт, присвячених методам вбудовування в молодший біт без суттєвого порушення закону розподілення бітів. Наприклад, тривіальною модифікацією методу LSB є LSB-*matching*, який випадковим чином змінює піксельні значення на ± 1 так, що молодші біти пік селів відповідають бітам повідомлення, що вбудовується. Завдяки такій модифікації LSB-*matching*

стеганоконтейнери набагато важче розпізнаються методами стеганоаналізу, але все рівно залишаються вразливими.

До сучасних стеганографічних методів висувається ряд вимог, серед яких найважливішими є: стійкість до пасивних та активних атак, забезпечення надійності сприйняття стегоконтейнера (око людини не може відрізнити контейнер від стего), забезпечення значної пропускної здатності прихованого каналу зв'язку. Треба зауважити, що одночасно усі вимоги забезпечити неможливо. Тому ефективність стегосистеми, що розробляється, розглядається виходячи із певного контексту.

Вбудовування інформації в контейнер призводить до зміни його характеристик. Чим менше таких змін зазнає контейнер тим важче стеганоаналітичним методам забезпечити низький рівень похибки при розпізнаванні. В останній час активно ведуться роботи по створенню стеганографічних методів та алгоритмів, розробники яких намагаються забезпечити найменш можливий вплив на контейнер вбудованої інформації як за рахунок вибору елементів контейнера для вбудовування так і специфіки самого алгоритму [1-5]. Однак, остаточного вирішення це питання не набуло, оскільки методи, які доступні з відкритих джерел, не мають строгого математичного підґрунтя, а отже не можуть бути універсальними.

Для побудови ефективної стеганографічної системи є важливим можливість апріорного забезпечення вимог щодо забезпечення надійності сприйняття та стійкості до стеганоаналізу.

Аналіз літератури

На сьогодні в літературі відсутнє строге формальне обґрунтування впливу модифікації того чи іншого елемента зображення - контейнера, на чутливість отриманого стеганоповідомлення до пасивних та активних атак.

Так у роботі [6] наведено результати експериментальних досліджень ефективності стеганоалгоритмів із використанням наборів тестових зображень з різним семантичним наповненням. Показано, що структурно-змістові особливості зображення суттєво впливають на ефективність приховування: зображення зі складною текстурою забезпечують вищу ємність і візуальну непомітність, тоді як гладкі однорідні області більш чутливі до внесених змін. Додатково оцінено стійкість прихованої інформації до дії атак JPEG-компресії, імпульсного шуму, фільтрації та геометричних трансформацій. Результати дослідження підтверджують, що підвищення ефективності стеганографічної системи можливе завдяки адаптивному вибору місця вбудовування, який враховує тип, семантику та статистичні характеристики зображення-контейнера. У роботі [7] формулюються вимоги до алгоритму пошуку елементів контейнеру для приховуваного вбудовування даних на основі методу найменш значущого біту. Для оцінки відповідності алгоритму пошуку щодо сформульованих вимог пропонується використовувати метрику, величина якої характеризує ступінь відмінності між результатами роботи алгоритму для двох різних контейнерів. Автор відмічає, що важливу роль для атакуючого відіграє чутливість до адаптивної зміни яскравості в залежності від діапазону, тобто семантична складова кожного окремого контейнеру є особливою, що значно ускладнює завдання підбору коефіцієнтів для алгоритму пошуку. Можливим варіантом розв'язання проблеми врахування семантичної складової є класифікація контейнерів по визначеним ознакам, наприклад: аерофотознімок земної поверхні, зображення будівель, ландшафту і т.д. В статті відзначається, що серед обмежень сформульованої системи вимог не враховується зміст інформаційного повідомлення, яке вбудовується.

Координати місця вбудовування повідомлення в роботі [8] запропоновано визначати на основі ітераційних функцій. Для передачі параметрів ітераційних функцій приймальній стороні застосовується алгоритм Діффі-Хеллмана.

В [9] питання вибору контейнера вирішується за допомогою двох крокової процедури. На першому кроці відбувається фільтрація потенційних контейнерів з врахуванням їх гістограм. На другому – аналізуються характеристики інтенсивності пікселей виділеного

© Борисенко І.І. Проблема вибору контейнера для забезпечення стійкості стего до збурних дій. Сучасний захист інформації, 1(65), 8–14.
https://doi.org/10.31673/2409-7292.2026.010115

блоку. Для підвищення ймовірності збереження надійності сприйняття стего проводяться додаткові геометричні перетворення, що забезпечує вирішення задачі, поставленої авторами, але не гарантує стійкості стего до збурних дій, а також робить алгоритм громіздким. В [10] розглядається вибір контейнера, стійкого до пасивних атак, акцент робиться на формати, в яких зберігаються зображення. Конкретний метод вибору контейнера в роботі не пропонується. В [11] вибір контейнера пропонується для одного стеганометода Бенгама-Мемона-Эо-Юнга, який автори попередньо модифікують, використовуючи замість ДКП вейвлет перетворення. В [12] множина контейнерів, з якої обирається кандидат на стегонографічний контейнер, містить не тільки зображення реального світу, а і створені штучно.

У роботі [13] було представлено метод, що базується на основі поняття обсягу захищеної інформації, що кількісно визначає об'єм вбудованої інформації, яка є захищеною від деякої збурної дії. Значною перевагою цього методу є відсутність обмежень на застосування стегнографічних алгоритмів і конкретики прогнозованих атак.

У роботі [14] запропоновано метод вибору стеганографічного контейнера на основі введеної кількісної характеристики, що характеризує об'єм інформації, яка буде правильно декодована після атаки на стеганоповідомлення, та обчислюється з врахуванням вектору розподілу вбудованої інформації серед власних векторів симетричної матриці контейнера та чутливості цих векторів до збурної дії, що відображає збурення від прогнозованої атаки на стеганоповідомлення. Цей метод базується на можливості представлення стеганоперетворення, тобто процесу вбудовування додаткової інформації, як деякої адитивної операції над матрицею зображення-контейнера.

В [15] представлено метод підвищення ефективності стеганосистеми шляхом модифікації методу вибору контейнера з поданої сукупності, на основі модифікації кількісної оцінки об'єму захищеної інформації, а саме використанням відносного значення об'єму захищеної інформації до об'єму всієї вбудованої інформації, запропонованого в [16].

На основі проведеного аналізу можна заключити, що недостатньо уваги в наукових дослідженнях приділено саме формальному дослідженню вибору елементів контейнера, які найменш чутливі до атак стеганоаналізу, і які забезпечать стійкість стегосистеми до збурних дій.

Мета та постановка задачі

Метою роботи є розробка метода оцінки збурень матриці контейнера при його стеганографічному перетворенні, який би не залежав від стеганографічного алгоритму, який використовується, і який дозволив би проводити порівняння збурень контейнера, які вносяться різними стеганоалгоритмами з метою вибору із доступної множини контейнерів такого, що задовольняв би заданим умовам.

Для досягнення мети потрібно вирішити задачі:

1) визначити математичний інструмент, за допомогою якого буде розроблятися метод;
2) дослідити збурення, які елемент контейнера вносить під час його модифікації з метою визначення кількісної міри для оцінки таких збурень;
3) побудувати функцію для оцінки збурень матриці контейнера при його стегоперетворенні;
4) провести обчислювальний експеримент з метою перевірки ефективності розробленого методу.

Основна частина

В якій би області (спектральній, просторовій, частотній) не проводилося стеганоперетворення (СП) матриці контейнера це обов’язково призведе до зміни значень елементів в просторовій області. Аналіз збурень контейнера показав, що в залежності від того значення яких елементів були модифіковані рівень збурення матриці контейнера буде неоднаковим. Розглянемо це ствердження у формальному вигляді.

В якості контейнера будемо використовувати цифрове зображення (ЦЗ) в градаціях сірого з матрицею $C=[c_{ij}]$ розмірності $m\times n$, $c_{ij}\in[0;255]$. Розглянемо два пікселі зі значеннями K_1 і K_2 таких, що $K_1>K_2$. Змінимо ці значення на +1 кожне (вибір такого значення продиктоване тим, що в багатьох випадках повідомлення представляється в бінарному вигляді), а значення інших пікселів залишимо без змін. Оскільки значення пікселів змінилися на однакову величину, то може здатися, що їх внесок у зміну характеристик контейнера повинен бути однаковим, але це не так. Так, наприклад, однією з важливих характеристик цифрового сигналу є його енергія [17]. Для ЦЗ енергія в просторовій області обчислюється за формулою: $E=\sum_i\sum_j c_{ij}^2$.

Тоді нове значення енергії $\overline{E}=E+\Delta E$ буде визначатися формулою: $\overline{E}=c_{11}^2+c_{12}^2+...+K_1^2+2K_1+1+...+K_2^2+2K_2+1+...+c_{mn}^2$.

Приріст функції $\Delta E=\delta 1+\delta 2$ складає сума величин $\delta 1=2K_1+1$ і $\delta 2=2K_2+1$, де $\delta 1>\delta 2$. Отже, внесок пікселя із значенням K_1 в ΔE більший, ніж внесок пікселя зі значенням K_2.

В наш час активно розвиваються методи стеганографії [18, 19 та інші], які базуються на загальному підході до аналізу стану й технології функціонування інформаційних систем (ЗПАІС) [20], в основу якого покладено матричний аналіз і теорія збурень. Перетворення контейнера за рахунок вкладення в нього повідомлення незалежно від способу і області цього вкладення, у відповідності до ЗПАІС представляється як збурення ΔC матриці C: $\overline{C}=C+\Delta C$, де $\overline{C}$ – матриця стеганоконтейнера або у вигляді сукупності збурень множини сингулярних чисел (СНЧ) і сингулярних векторів (СНВ) матриці контейнера, які її однозначно визначають. Нагадаємо, що для матриці C сингулярне перетворення (SVD) має вигляд: $C=U\Sigma V^T$, де U, V – ортогональні матриці, (тобто $U^TU=I$, $V^TV=I$, I – одинична матриця) розмірності $m\times n$ і $n\times n$ відповідно; $\Sigma=diag(\sigma_1,...,\sigma_n)$, $\sigma_1\ge...\ge\sigma_n\ge 0$. Стовпці $u_1,...,u_n$ матриці U і $v_1,...,v_n$ матриці V називають відповідно лівими і правими сингулярними векторами матриці C, величини $\sigma_1,...,\sigma_n$ – сингулярними числами.

Оскільки СНЧ і СНВ є параметрами, які однозначно характеризують матрицю контейнера [20], то в якій би області перетворення контейнера не відбулися зміни, ці зміни відобразяться на СНЧ и СНВ.

В [21] одержана формула енергії зображення, яка виражається через СНЧ матриці контейнера, а саме: $E=\sigma_1^{\,2}+...+\sigma_n^{\,2}$, тобто енергія матриці контейнера дорівнює сумі квадратів СНЧ. Таким чином, справедлива рівність $E=\sum_i\sum_j c_{ij}^2=\sigma_1^2+\sigma_2^2+...+\sigma_n^2$, а це означає, що величини $\delta 1$ і $\delta 2$ обов'язково відобразяться в сингулярному спектрі матриці контейнера. Норма матриці збурень $\|\Delta C\|_2$ не залежить від того, які саме СНЧ були збурені при СП, а залежить тільки від абсолютних величин цих збурень, тому в подальшому будемо використовувати саме СНЧ.

Як було показано вище, різні елементи вносять різний внесок в загальний рівень збурень контейнера, тому пропонується зробити попередню обробку контейнера з метою визначення коефіцієнтів μ_{ij} – кількісної оцінки внеску кожного елемента c_{ij} контейнера в $\|\Delta C\|_2$. Збурення елементів контейнера будемо моделювати зміною їх значень на найменш можливе, а саме на одиницю.

Основні кроки обчислення μ_{ij} і його використання:

1) збурити елемент c_{ij}, в результаті одержуємо матрицю $\overline{C}_{\sim ij}$, в якій значення усіх елементів співпадає із значеннями елементів матриці C, окрім одного, значення якого змінилося на одиницю;

© Борисенко І.І. Проблема вибору контейнера для забезпечення стійкості стего до збурних дій. Сучасний захист інформації, 1(65), 8–14.
https://doi.org/10.31673/2409-7292.2026.010115

2) для матриць C і $\overline{C}_{\sim ij}$ побудувати сингулярний розклад: $C = USV^T$, $\overline{C}_{\sim ij} = \overline{U}_{\sim ij}\overline{S}_{\sim ij}\overline{V}^T_{\sim ij}$;

3) знайти збурення матриці СНЧ: $\Delta S = S - \overline{S}_{\sim ij}$;

4) оцінити значення μ_{ij} за формулою $\mu_{ij} = \max_i |\Delta S_{ii}|$, де ΔS_{ii} – діагональні елементи матриці ΔS.

5) елементи контейнера, для яких виконується умова $\mu_{ij} \in [(\mu_{ij})_{\min}; P]$, використовувати для вбудовування повідомлення (P – деяке значення μ_{ij}, яке визначається виходячи з об'єму повідомлення);

6) для оцінки збурень контейнера внаслідок СП використовувати функцію $FS = \sum_{\mu_{ij} \in [(\mu_{ij})_{\min}; P]} \mu_{ij}$.

Розглянемо декілька додатків використання коефіцієнтів μ_{ij}.

Одним з відкритих питань є порівняння ефективності стеганографічних алгоритмів. Для порівняння декількох стеганографічних алгоритмів $CA_1, ..., CA_n$ по критерію збурень матриці контейнера, потрібно визначити елементи, в яких локалізовано повідомлення для кожного з CA_i та виконати пункти 1) – 4). Для кожного з CA_i обчислити $FS_1 = \sum_{локализ.CA1} \mu_{ij}$, …, $FS_n = \sum_{локализ.CAn} \mu_{ij}$. Порівняння FS_i провести виходячи з того, що чим менші збурення були внесені в контейнер внаслідок СП, тим FS_i будуть меншими.

Для перевірки ефективності запропонованого метода алгоритмом CA_i модифікувалися елементи контейнера, яким відповідали найменші μ_{ij} (область I), а потім алгоритмом CA_i – усі інші елементи (область II). Одержані результати наведені в таблиці 1.

Таблиця 1

Порівняльна характеристика збурень контейнера після СП

Об'єм вбудованого повідомлення	область I		область II	
	FS	$\|\Delta C\|_2$	FS	$\|\Delta C\|_2$
10 бітів	0,1903	1,4142	1,3362	2,1358
1/5 контейнера	32,4363	34,6888	85,9742	45,3085
1/2 контейнера	160,9376	49,3305	212,4801	65,8341

В [22] був запропонований стеганографічний алгоритм GRAPH_*matching*, в основу якого покладено побудову графової моделі контейнера. Цим алгоритмом вбудовування повідомлення відбувається за рахунок обміну елементів контейнера в більшій мірі, ніж за рахунок їх модифікації, що дозволяє зберегти статистики першого порядку. Елементи контейнера розбиваються на групи і кожній такій групі ставиться у відповідність вузол графа. Ребра між вузлами створюються тільки в тому випадку, якщо елемент одного вузла можна обміняти на елемент іншого без видимого спотворення контейнера. Оскільки вузли – це групи елементів, то ребер між вузлами може бути декілька, отже, може існувати декілька пар елементів, які можна обміняти. Цю ситуацію, з врахуванням описаного вище метода, будемо використовувати таким чином. Виконати попередню обробку контейнера, в результаті чого одержимо матрицю M коефіцієнтів μ_{ij}. Якщо вузлу інцидентно декілька ребер, то для обміну елементів c_{ij} і c_{kl} контейнера вибрати ту пару, якій відповідає найменша сума $\mu_{ij} + \mu_{kl}$.

Оцінка збурень контейнера, які відбулися внаслідок СП алгоритмом GRAPH_*matching* і його модифікованою версією GRAPH_*matching_1* наведено в таблиці 2.

© Борисенко І.І. Проблема вибору контейнера для забезпечення стійкості стего до збурних дій. Сучасний захист інформації, 1(65), 8–14.
https://doi.org/10.31673/2409-7292.2026.010115

Таблиця 2

Порівняльна характеристика збурень контейнера $\|\Delta C\|_2$

Об'єм вбудованого повідомлення	GRAPH *matching 1*	GRAPH *matching*
10 бітів	0,4142	1,9358
1/5 контейнера	32,6878	46,3185
1/2 контейнера	50,5305	68,7341

Висновки

У роботі запропоновано метод оцінки збурень контейнера, який дозволяє мінімізувати ці збурення за рахунок визначення місця локалізації повідомлення, що вбудовується. Запропонований метод може використовуватися при розробці нових стеганографічних алгоритмів, а також для порівняння різних стеганоалгоритмів з метою вибору кращого з них по критерію мінімальності збурень, які вносяться у контейнер. Попередня обробка контейнера дозволяє вибрати із множини доступних контейнерів той, кількість елементів якого з малими коефіцієнтами μ_{ij} відповідно бажаному порогу задовольняє бажаний об'єм.

Зауважимо, що координати пікселей, які обираються для вбудовування повідомлення, являються ключем і таких координат, в залежності від об'єму повідомлення, може бути досить велика кількість, тобто виникає проблема передачі і розподілення ключів. Цю проблему можна вирішити, наприклад, методом запропонованим авторами у [8].

Перелік посилань

1. Filler T., Judas J., Fridrich J. Minimizing Additive Distortion in Steganography Using Syndrome-Trellis Codes. Forensics and Security. 2011. Vol. 6(1). P. 920–935. https://doi.org/10.1109/TIFS.2011.2134094.

2. Kodovský J., Fridrich J., Holub V. On Dangers of Overtraining Steganography to an Incomplete Cover Model. Proc. ACM Multimedia & Security Workshop, Niagara Falls, New York, September 29-30.2011. P. 69-76. Latest updates: https://dl.acm.org/doi/10.1145/2037252.2037266.

3. Filler T., Fridrich J. Gibbs construction in Steganography. Forensics and Security.2010. Vol. 5(4). P. 705-720. http://dde.binghamton.edu/filler/pdf/fill10tifs-gibs-journal.pdf.

4. Fridrich J., Filler T. Practical methods for minimizing embedding impact in steganography Proceedings SPIE. Electronic Imaging, Steganography, and Watermarking of Multimedia Contents IX. 2007.P. 2-3. https: // www. spiedigitallibrary.org/conference-proceedings-of-spie/6505/1/Practical-methods-for-minimizing-embedding-impact-in-steganography steganography/10.1117/12.697471.full.

5 Hetzl S., Mutzel P. A graph-theoretic approach to steganography. Proc. Communication and Multimedia security. 2005. P.119-128. https://dmg.tuwien.ac.at/hetzl/research/graphstego.pdf.

6. Журавель Ю.І., Мичуда Л.З., Сколоздра М.М. Оцінювання впливу семантики зображень на ефективність стеганографічних методів. Сучасний захист інформації. 2025. № 4(64). С 73-80. DOI: 10.31673/2409-7292.2025.041208.

7. Бекіров А.Е. Формулювання вимог до алгоритму пошуку елементів просторового представлення контейнеру для стеганографічного вбудовування. Теоретичні основи розробки та експлуатації систем озброєння. 2021. С. 32-36 DOI: 10.30748/soivt.2021.66.04.

8. Журавель І.М., Мичуда Л.З., Журавель Ю.І. Підвищення ефективності стеганографічного методу приховування даних із застосуванням ітераційних функцій та додаванням шуму. Український журнал інформаційних технологій. 2021. т.3, №2. С. 68-73. doi.org/10.23939/ujit2021.02.066.

9. Abed S., Al-Roomi S.A., Al-Shayeji M. Efficient cover image selection based on spatial block analysis and DCT embedding. EURASIP Journal on Image and Video Processing. 2019.P. 87. doi: 10.1186/s13640-019-0486-8.

10. Mustafayeva E. Principles of Choosing Containers for Steganographic Systems. International Journal of 3D Printing Technologies and Digital Industry. 2020. vol.4, no. 3, P. 264-229.

11. Nikishova A.V., Omelchenko T.A., Makedonskij S.A. Steganographic embedding in containers-images. Journal of Physics: Conference Series. 2018. vol. 1015, no. 4. doi: 10.1088/1742-6596/1015/4/042041.

12. Li, X., Guo, D., Qin, C. Diversified Cover Selection for Image Steganography. Symmetry 2023. 15, 2024. https://doi.org/10.3390/sym15112024

13. Kobozeva A.A., Narimanova E.V. Stegoimage disturb sensitivity estimate. System Research and Information Technologies. 2008. No. 3. P. 52-65.

© Борисенко І.І. Проблема вибору контейнера для забезпечення стійкості стего до збурних дій. Сучасний захист інформації, 1(65), 8–14.
https://doi.org/10.31673/2409-7292.2026.010115

14. Надвоцький О.Ю., Кобозєва А.А. Метод розв'язку задачі про вибір контейнера, що забезпечує малу чутливість стеганоповідомлення до збурних дій. http: // immm.op.edu.ua / files / archive / n3_v11_2021/immm_ n3_ v11_2021.pdf.

15.Сокальський С. М. Модифікація методу вибору контейнера для зменшення чутливості стеганоповідомлення до збурних дій. Informatics and Mathematical Methods in Simulation Vol.13 (2023), No. 3-4, pp. 311-321 http://immm.op.edu.ua/files/archive/n3-4_v13_2023/2023_3-4(14).pdf.

16. Bobok I., Kobozieva A., Sokalsky S. The Problem of Choosing a Steganographic Container in Conditions of Attacks against an Embedded Message. https://journal.ie.asm.md/assets/files/07_04_56_2022.pdf.

17. Gonzalez R., Voods R. Digital image processing. 3nd ed. NJ: Pearson, 2018. https: // www.cl72.org/ 090image-PLib/books/Gonzales, Woods-Digital.Image.Processing.4th.Edition.pdf.

18. Борисенко І.І. Застосування методів порівняння послідовностей в стеганографічних перетвореннях цифрових зображень. Сучасна спеціальна техніка. 2014. №2(37). С. 110 -115. https://suchasnaspectehnika.com /journal/ukr/2020_2/3.pdf.

19. Борисенко І.І. Метод оцінки збурень контейнера внаслідок його стеганографічного перетворення.10 МНПК Військова освіта і наука: сьогодення та майбутнє. 2014. https: // suchasnaspectehnika.com / journal / ukr / 2020_2/3.pdf.

20. Кобозева А.А. Загальний підхід до оцінки властивостей стеганографічного алгоритму, заснованого на теорії збурень. Информационные технологии и компьютерная инженерия. 2008.№1(11).С.164-171.

21. Кобозева А.А., Борисенко И.И. Повышение помехоустойчивости стеганографических методов, использующих сингулярное и спектральное разложение матрицы контейнера. Труды одесского политехнического университета.2007. №2(28). С. 192-198. https: // old-pratsi.op.edu.ua / app / webroot / articles / 1312737920.pdf.

22. Борисенко І.І. Застосування теорії графів в задачах створення стеганографічних повідомлень. Сучасна спеціальна техніка. 2015. №2. С. 26-33.

Надійшла до редакції (Received): 10.01.2026
Прийнята до друку (Accepted): 17.03.2026
Опубліковано онлайн (Available online): 30.03.2026

УДК 004.056:[004.032.26+519.17
DOI: 10.31673/2409-7292.2026.010224

Гашко А.О., Ананченко О.Є.

ГРАФОВІ НЕЙРОННІ МЕРЕЖІ ДЛЯ ПРОТИДІЇ ВІДМИВАННЮ КОШТІВ У КРОСЧЕЙН-БЛОКЧЕЙН СЕРЕДОВИЩАХ

Поширення кросчейн-мостів та рішень агрегації другого рівня (Layer-2) принципово трансформувало структуру блокчейн-транзакційних мереж, одночасно створивши нові канали для протиправної фінансової активності, що уникає традиційних механізмів протидії відмиванню коштів (AML). Ранні спроби використання науки про дані для блокчейн-аналітики, зокрема методів кластеризації та розпізнавання шаблонів на великих наборах даних, заклали необхідне підґрунтя для розуміння аномальної поведінки у децентралізованих реєстрах – що підтверджується попередньою роботою з порівняння алгоритмів кластерного моделювання на великих даних, отриманих із записів розподілених реєстрів (наприклад, порівняння алгоритмів побудови кластерних моделей на блокчейн-похідних наборах даних. Однак ці попередні методології здебільшого обмежувалися офлайн-аналізом і статичними парадигмами кластеризації. У цій статті ми розвиваємо це базове дослідження, пропонуючи фреймворк на основі графових нейронних мереж (GNN) для оцінювання AML-ризиків у реальному часі в межах кількох гетерогенних блокчейн-мереж. На відміну від ранніх кластероцентричних підходів, запропонована модель будує єдиний темпоральний кросчейн-граф, який інтегрує внутрішньомережеву активність, взаємодії через кросчейн-мости та події розрахунків Layer-2 в узгоджену структуру. Архітектура GNN із передаванням повідомлень використовується для навчання інформативних ембедингів вузлів, що відображають реляційні залежності та часову динаміку між мережами, із застосуванням механізмів часового згасання та зважування типів ребер для підвищення чутливості до відкладених і фрагментованих тактик відмивання. Ми виводимо ймовірнісну функцію ризикового скорингу на основі навчених ембедингів і оптимізуємо модель за допомогою композитної функції втрат, яка балансує якість класифікації, гладкість графа та часову стабільність. Фреймворк оцінено на реальних даних мереж Ethereum, BNB Chain, Solana та TON, що охоплюють кросчейн-перекази, депозити та P2P-

© Борисенко І.І. Проблема вибору контейнера для забезпечення стійкості стего до збурних дій. Сучасний захист інформації, 1(65), 8–14.
https://doi.org/10.31673/2409-7292.2026.010115