Оцінка підходу продемонструвала надійну продуктивність, забезпечивши точність 0,934, повноту 0,948, F_1 0,841 та AUC 0,872. У порівнянні з існуючими аналогами, запропонований метод показав послідовні покращення за ключовими показниками: точність збільшилася на 0,130%, F_1-оцінка покращилася на 0,031, а AUC зросла на 0,132.

Ключова технічна інновація полягає у використанні відносних, а не абсолютних позиційних вбудовувань у нейронну архітектуру. Це дозволяє моделі фіксувати нюансовані зв'язки між словами залежно від їх контекстного зміщення, тим самим підвищуючи її чутливість до тонких текстових сигналів, які часто сигналізують про прояви ПТСР. Також, покращена диференціація від інших психічних розладів була забезпечена шляхом розширення набору даних, щоб включити зразки, що відображають прояви альтернативних психологічних станів, які були розміщені в ортогональній референтній категорії. Це рішення допомогло моделі вивчити чіткіші межі між специфічним для ПТСР контентом та симптомами, що вказують на інші психічні захворювання.

Ключові слова. *Посттравматичний стресовий розлад, NLP, нейромережа, текстові дані*

УДК 004.056.5
DOI https://doi.org/10.36059/978-966-397-538-2-4

НОРМОВАНА ВІДОКРЕМЛЕНІСТЬ МАКСИМАЛЬНОГО СИНГУЛЯРНОГО ЧИСЛА БЛОКУ ЦИФРОВОГО ЗОБРАЖЕННЯ ЯК ПОКАЗНИК ДОЦІЛЬНОСТІ ЙОГО СТЕГАНОПЕРЕТВОРЕННЯ

Dr.Sci. І. Бобок[1][0000-0003-4548-0709], **Dr.Sci. А. Кобозєва**[2][0000-0001-7888-0499]

[1]Національний університет «Одеська політехніка», Україна,
[2]Одеський національний морський університет, Україна,
EMAIL: [1]onu_metal@ukr.net, [2]alla_kobozeva@ukr.net

Анотація. *Одним із найбільш перспективних та ефективних напрямів захисту інформації сьогодні є стеганографія. Серед низки вимог до стеганосистеми одною з основних є забезпечення надійності сприйняття стеганоповідомлення. Однак багато існуючих стеганометодів, зокрема стійких до атак проти вбудованого повідомлення, не в змозі систематично забезпечувати ацю вимогу та не розраховані на роботу з випадковим контейнером, який на практиці є найчастіше застосовуваним. Метою роботи є підвищення ефективності стеганосистеми при використанні довільного стеганометоду і випадкового контейнеру шляхом розробки методу вибору блоків контейнера, в якості якого використовується цифрове*

зображення, для вбудови в них додаткової інформації. Критерієм ефективності виступає надійність сприйняття формованого стеганоповідомлення, що кількісно оцінюється за допомогою різницевого показника - пікового відношення «сигнал-шум». Мета була досягнута шляхом дослідження властивостей формальних параметрів блоків цифрового зображення – сингулярних чисел з урахуванням відповідності сингулярних трійок і частотних складових блоку. Найбільш важливим результатом роботи є теоретично обґрунтоване визначення параметра блоку, що дає інтегральну кількісну характеристику відносного розподілу його частотних складових – нормованої відокремленості максимального сингулярного числа блоку. Практична значимість отриманих результатів полягає в розробці методу вибору блоків зображення і методу визначення небажаних для використання в якості контейнера зображень, алгоритмічні реалізації яких дозволили підвищити ефективність стеганосистеми при їх застосуванні.

***Ключові слова**: стеганографія, цифрове зображення, надійність сприйняття стеганоповідомлення, вибір блоку контейнера, вибір контейнера, нормована відокремленість сингулярного числа.*

Вступ

Стеганографічна система сьогодні є одною з напотужніших систем захисту інформації, яка дає можливість приховати сам факт наявності секретного повідомлення шляхом його попереднього кодування, в результаті чого отримується додаткова інформація (ДІ), і вбудови в деякий інформаційний об’єкт – контейнер, що не привертає уваги, в якості якого в сучасних умовах найчастіше використовується цифрове зображення (ЦЗ) [1], що і розглядається в роботі. Результатом вбудови ДІ є стеганоповідомлення (СП).

До стеганографічної системи висувається низка вимог, серед яких: стійкість до виявлення (стеганоаналізу [2,3]); стійкість до атак проти вбудованого повідомлення [4] – збурних дій (ЗД), які змінюють матрицю СП; забезпечення надійності сприйняття СП (зміни, що вносяться при вбудові ДІ не повинні бути помітними); значна пропускна спроможність прихованого каналу зв’язку; можливість забезпечення автентифікації [5]; незначної обчислювальної складності тощо [6]. Одночасне задоволення всіх цих вимог викликає труднощі, адже задоволення деяких з них вимагає виконання взаємовиключних умов. Так відомо [7], що модифікація високочастотних складових веде до найменших візуальних спотворень вихідного зображення. Однак застосування даного факту на практиці в області стеганографії не завжди виправдано в силу того, що при використанні для вбудови ДІ високочастотної складової зображення одержуване СП виявиться чутливим до будь-яких атак проти вбудованого повідомлення, що змушує шукати інші, компромісні можливості забезпечення необхідних властивостей. Ще одним прикладом взаємовиключних вимог на практиці можна вважати забезпечення якнайбільшої пропускної спроможності прихованого каналу і надійності сприйняття СП, оскільки зі збільшенням пропускної спроможності, як

правило, ймовірність непомітності спотворень в результаті стеганоперетворення (СПр) зменшується [1].

Враховуючи вищезазначене, на практиці до уваги беруться конкретні, передбачувані, умови використання конкретної стеганографічної системи, з оглядом на які формуються пріоритети вимог до стеганосистеми [8].

На сьогодні актуальною, такою, що не має остаточного рішення, залишається задача систематичного забезпечення надійності сприйняття СП, зокрема при використанні стеганографічних методів, стійких до атак проти вбудованого повідомлення. Відомо [9], що для того, щоб існувала потенційна можливість декодування ДІ зі СП, що піддалось ЗД, збурення контейнера в результаті вбудови ДІ повинно бути не менше, ніж збурення, що є результатом атаки на СП. Враховуючи це, очевидно, що для забезпечення стійкості СП до значних ЗД спотворення контейнера при СПр, як правило, будуть більшими, ніж коли задача забезпечення стійкості до атак проти вбудованого повідомлення не є критичною. Це означає, що для стійких стеганоалгоритмів задача забезпечення надійності сприйняття СП є більш актуальною і потребує більших зусиль для її рішення, ніж для стеганоалгоритмів, від яких стійкість не вимагається. Саме цій задачі і присвячена дана робота.

Аналіз проблеми

Питання розробки достатніх умов забезпечення надійності сприйняття, стійкості СП до ЗД не раз піднімалися вченими-стеганографами. Так в [9] на основі загального підходу до аналізу стану інформаційних систем (ЗПАІС) було доведено, що з метою забезпечення значної ймовірності надійності сприйняття СП вбудову ДІ в ЦЗ-контейнер доцільно робити таким чином, щоб збурені в результаті СПр сингулярні вектори (СНВ) матриці контейнера відповідали малим за значенням сингулярним числам (СНЧ); збурення будь-яких СНЧ були незначними. Для забезпечення стійкості стеганосистеми до атак проти вбудованого повідомлення достатньо, щоб в процесі вбудови ДІ збурення отримали нечутливі до ЗД параметри повного набору матриці контейнера, який складається з СНВ і СНЧ, що визначаються однозначно для матриці ЦЗ шляхом застосування нормального сингулярного розкладання [10]. Отримані достатні умови є загальними, можуть бути застосованими незалежно від того, в якій області ЦЗ-контейнера (просторовій, перетворення) відбувається СПр, але їх одночасне застосування є утрудненим, оскільки, зокрема, нечутливі до збурних дій СНВ відповідають найбільшим за значенням СНЧ, що суперечить достатній умові надійності сприйняття. Аналогічне зауваження може бути висунутим до достатніх умов, отриманих в [11] в області перетворення Уолша-Адамара шляхом використання ЗПАІС, на основі якого були встановлені зв’язки між трансформантами Уолша-Адамара, коефіцієнтами дискретного косинусного перетворення і складовими сингулярного розкладання відповідних матриць.

Однак усі достатні умови вимагають їхнього врахування під час розробки стеганографического методу. Для наявних методів задоволення існуючим достатнім умовам вимагає, як правило, їхньої певної модифікації або взагалі не може бути реалізованим, хоча надійність сприйняття, стійкість до атак такими методами може і не забезпечуватися систематично, як, наприклад, методом, запропонованим в [4], який до цього моменту залишається одним з найбільш стійких до атаки стиском з малими коефіцієнтами якості, але не забезпечує систематично надійність сприйняття формованого СП.

Модифікація методу не є тривіальним питанням. Вона вимагає змін математичного базису, змін в практичній реалізації, при цьому будь-яка модифікація методу, спрямована на поліпшення конкретної властивості, може погіршити інші показники методу. З урахуванням цього бажаним є пошук можливості поліпшення результатів застосування стеганометоду, розширення області його застосування без будь-якої модифікації.

Усі контейнери, що використовуються в стеганографії, можна розділити на три класи: обрані, випадкові та нав'язані [12]. Саме вибір контейнера дозволяє найкраще забезпечити необхідні властивості СП, але на практиці найчастіше контейнер є випадковим, наслідком чого є бажаність незалежності властивостей стеганоалгоритму від властивостей контейнера. Однак багато наявних стеганографічних методів не розраховані на випадковий контейнер, маючи обмеження на область застосування, що очевидно є їх недоліком [8,13]. Так в [14] запропонований стійкий до атак проти вбудованого повідомлення метод, що робить вбудову ДІ в просторовій області ЦЗ-контейнера шляхом певних збурень яскравості пікселів. Цей метод не гарантує забезпечення надійності сприйняття СП, що зазначається одним з авторів в [15], де пропонується його модифікація, яка теж не вирішую проблему остаточно.

Більшість сучасних стеганометодів, зокрема розглянуті вище, є блоковими [16,17], що дозволяє: краще забезпечити їх стійкість до атаки стиском; порівняно незначну обчислювальну складність, оскільки тут, незалежно від конкретики способу обробки окремого блоку, для матриці розміром $n \times n$ вона становить $O(n^2)$ операцій, тобто визначається кількістю непересічних блоків; можливість розпаралелювання тощо. Очевидно, що блоки в межах одного ЦЗ розрізняються по своїх властивостях і вибір серед них для вбудови ДІ принципово може забезпечити певні вимоги до СП навіть при випадковому контейнері, тобто є тим джерелом, при використанні якого існує принципова можливість забезпечити надійність сприйняття СП для довільного стеганометоду, навіть стійкого до атак проти вбудованого повідомлення, для випадкового ЦЗ-контейнера.

Метою роботи є підвищення ефективності стеганографічної системи при використанні довільного стеганометоду і випадкового контейнеру шляхом розробки методу вибору блоків ЦЗ-контейнера для СПр.

Під ефективністю стеганосистеми в роботі розуміється ступінь забезпечення надійності сприйняття СП, яка кількісно оцінюються

стандартним для стеганографії чином – різницевим показником *PSNR* - піковим відношенням «сигнал-шум» [1].

Звичайно, будь-який вибір блоків контейнера потенційно зменшує можливу пропускну спроможність формованого прихованого каналу зв'язку, але, по-перше, такий вимушений захід дасть можливість для використання існуючих ефективних методів без будь-яких їх модифікацій в умовах випадкового контейнера, по-друге, з урахуванням бурхливого розвитку стеганоаналітичних методів використання стеганометодів в умовах малої пропускної спроможності стеганоканалу є поширеною сучасною тенденцією [18].

Для досягнення поставленої мети в роботі розв'язуються наступні *задачі*:

1. Визначення параметра блоку матриці ЦЗ, що дає кількісну характеристику розподілу його частотних складових незалежно від формату збереження (з/без втрат) зображення;
2. Розробка методу вибору блоків ЦЗ-контейнера для СПр, заснованого на аналізі нормованої відокремленості максимального СНЧ блоку;
3. Розробка методу вибору ЦЗ-контейнера для підвищення ефективності довільного стеганометоду без його модифікації.

Інтегральний показник розподілу частотних складових блоку цифрового зображення

При вбудові ДІ для забезпечення різноманітних властивостей отримуваного СП важливим є те, які саме збурення отримують в результаті СПр формальні параметри контейнера, зокрема частотні коефіцієнти, параметри сингулярного розкладання відповідної матриці тощо, та локалізація цих збурень.

Нехай F – $n\times n$-матрица ЦЗ-контейнера, що піддається розбивці на непересічні $l\times l$-блоки $B_{ij}, i, j = \overline{1,\lceil n/l \rceil}$, стандартним чином [7], де $\lceil\cdot\rceil$ - ціла частина аргументу. Блоки мають різні властивості в межах одного ЦЗ, зокрема мають різний вміст частотних складових. Як вже зазначалося вище, при окремому розгляді одних з основних вимог до СП, а саме забезпечення надійності сприйняття та нечутливості до ЗД, для забезпечення першої бажаним є задіювання в процесі вбудови ДІ високочастотної складової, в той час, як для забезпечення стійкості пріоритет має низькочастотна складова. Одночасне максимальне задоволення цих вимог є неможливим, але для досягнення певного компромісу бажаним є визначення (при можливості) такого параметру, який би давав інтегральну характеристику ступеня вмісту різних частот у конкретний блок. Саме такий параметр при його використанні дасть змогу для вибору шуканих блоків для СПр з потрібним співвідношенням частотних складових.

В якості такого інтегрального параметру з урахуванням результатів досліджень, проведених в [19,20], пропонується використовувати нормовану відокремленість максимального СНЧ блоку (НВМСЧ) ЦЗ. Покажемо, що її значення є загальним показником вмісту частотних складових в блок.

Нехай

$$B = U\Sigma V^T \quad (1)$$

- нормальне сингулярне розкладання блоку *B* деякого ЦЗ [10], де *U, V* – ортогональні матриці, стовпці яких u_i, v_i , $i = \overline{1,l}$, є лівими і правими СНВ відповідно, при цьому ліві СНВ є лексикографічно додатними, $\Sigma = diag(\sigma_1(B),..., \sigma_l(B))$,

$$\sigma_1(B) \geq ... \geq \sigma_l(B) \geq 0 \quad (2)$$

– СНЧ *B*, $(\sigma_i(B), u_i, v_i)$, $i = \overline{1,l}$, - сингулярні трійки. Для блоків оригінального ЦЗ, незалежно від формату збереження (з/без втрат) співвідношення (2) можна уточнити:

$$\sigma_1(B) >> \sigma_2(B) \geq ... \geq \sigma_l(B) \geq 0 . \quad (3)$$

Нормальнее сингулярне розкладання в умовах відсутності кратних СНЧ визначається однозначно [10] на відміну від звичайного [21].

Між сингулярними трійками і частотними складовими (блоків) ЦЗ існує певна відповідність [9]: сингулярні трійки, що містять максимальні/ мінімальні/ середні за значенням СНЧ, несуть в собі, головним чином, інформацію про низькочастотну/високочастотну/середньочастотну складові *B*, але і всі інші частотні складові в різних співвідношеннях будуть присутніми в кожній матриці $\sigma_i(B)u_i v_i^T$, що є доданком в сингулярному розкладанні в формі зовнішніх добутків [21]: $B = U\Sigma V^T = \sum_{i=1}^{l} \sigma_i(B) u_i v_i^T$. При цьому саме СНЧ в цих трійках є відповідальними за основну частотну складову блока. Це випливає з наступного [9]. Енергія E (*B*) *l*×*l*-блоку *B* ЦЗ визначається у відповідності з формулами: $E(B) = \sum_{u=0}^{l-1} \sum_{v=0}^{l-1} P(u,v) = \sum_{i=1}^{l} \sigma_i^2(B)$, де $P(u,v), u = \overline{0,l-1}, v = \overline{0,l-1}$, - енергетичний спектр *B*. Для блоків ЦЗ чим менше високочастотна/низькочастотна складова, тим більше/менше перше СНЧ відрізняється від всіх інших у відповідності з (3) [19,20]. Таким чином, ступінь цієї відмінності можна розглядати як показник вмісту певних частотних складових у блок ЦЗ. Але сингулярні спектри блоків дуже розрізняються між собою. Так, наприклад, якщо розглянути два 8×8-блоки ЦЗ (рис.1(а) – місця розташування блоків позначені червоними стрілками), то їх сингулярні спектри визначаться наступним чином:

897.7032, 15.2044, 4.5597, 2.9882, 1.7688, 1.6169, 0.5087, 0.3562;
1.0e+003 *1.3086, 0.0655, 0.0137, 0.0057, 0.0029, 0.0022, 0.0017, 0.0007. (4)

Очевидно, що співвідношення між значеннями СНЧ різних блоків можуть настільки відрізнятися між собою, що встановити по них порівняне співвідношення між вмістом високо/низько/середньочастотних складових для

різних блоків буде складно. Але картина стає більш зрозумілою після нормування сингулярного спектру. Позначимо $\sigma = (\sigma_1(B), \sigma_2(B), ..., \sigma_l(B))^T$ - вектор сингулярного спектру блоку *B*; $\overline{\sigma} = \sigma / \|\sigma\|$ - нормований вектор СНЧ, де $\|\sigma\|$ норма σ. Для $\overline{\sigma}$ відносні співвідношення між СНЧ є очевидними, оскільки всі його елементи належать одній множині – сегменту [0,1]. Показником ступеня відмінності $\sigma_1(B)$ від інших СНЧ блоку, а тому кількісною характеристикою внеску певних частот в блок, виступає нормована відокремленість $\sigma_1(B)$. Нормована відокремленість $svdgap_n(i)$ СНЧ $\sigma_i(B)$ визначається у відповідності з формулою [19,20]: $svdgap_n(i) = \min\limits_{i \neq j} \left| \overline{\sigma}_j - \overline{\sigma}_i \right|$, де $\overline{\sigma}_i$, $i = \overline{1,l}$ - компоненти вектора $\overline{\sigma}$. Тоді:

$$svdgap_n(1) = \overline{\sigma}_1 - \overline{\sigma}_2, \qquad (5)$$

При цьому $svdgap_n(1) \in]0,1]$. Значення нуля виключається з можливих для $svdgap_n(1)$ завдяки (3).

Враховуючи [20], можна зробити висновок, що чим ближче $svdgap_n(1)$ до одиниці, тим більшою є ступінь відносного перевищення $\overline{\sigma}_1$, а тому і $\sigma_1(B)$ всіх інших СНЧ блоку, тим менше їх відносний внесок в сингулярний спектр (в енергію блоку), тим більше/менше відносний вклад низькочастотної/ високочастотної складової в цей блок. Для розглянутого вище приклада блоків з сингулярними спектрами (4), відповідні вектори $\overline{\sigma}$ мають вигляд:

0.9998, 0.0169, 0.0051, 0.0033, 0.0020, 0.0018, 0.0006, 0.0004;
0.9987, 0.0500, 0.0105, 0.0043, 0.0022, 0.0017, 0.0013, 0.0006,

При цьому для першого з блоків $svdgap_n(1)$=0.9829, тоді як для другого $svdgap_n(1)$=0.9487, тобто на 4% менше, що говоре про другий блок як такий, вміст високочастотної складової в який є відносно більшим, ніж в перший, що повністю відповідає реаліям, які чітко прослідковуються по матрицях блоків:

$$\begin{pmatrix} 81 & 98 & 109 & 111 & 111 & 116 & 121 & 129 \\ 83 & 103 & 108 & 110 & 113 & 117 & 121 & 127 \\ 85 & 101 & 108 & 110 & 114 & 118 & 121 & 126 \\ 88 & 102 & 108 & 109 & 114 & 119 & 122 & 127 \\ 89 & 103 & 107 & 110 & 116 & 120 & 123 & 127 \\ 91 & 106 & 106 & 110 & 116 & 119 & 122 & 127 \\ 93 & 109 & 108 & 111 & 116 & 120 & 123 & 127 \\ 96 & 112 & 108 & 109 & 116 & 120 & 125 & 129 \end{pmatrix}, \begin{pmatrix} 103 & 148 & 167 & 176 & 178 & 179 & 176 & 166 \\ 106 & 153 & 166 & 176 & 178 & 180 & 179 & 174 \\ 110 & 155 & 169 & 175 & 178 & 182 & 179 & 176 \\ 112 & 157 & 168 & 175 & 179 & 181 & 178 & 175 \\ 115 & 160 & 171 & 175 & 179 & 178 & 174 & 166 \\ 120 & 162 & 172 & 175 & 178 & 177 & 153 & 131 \\ 124 & 163 & 171 & 177 & 177 & 176 & 151 & 127 \\ 129 & 165 & 169 & 178 & 179 & 174 & 151 & 141 \end{pmatrix},$$

Тут очевидним є більш значний перепад значень яскравості для другого блоку, який говоре про наявність контурів об'єктів, що локалізуються в області першого і другого стовпців, а також 6-го, 7-го і 8-го стовпців в області рядків з тими ж номерами, в межах цього блоку.

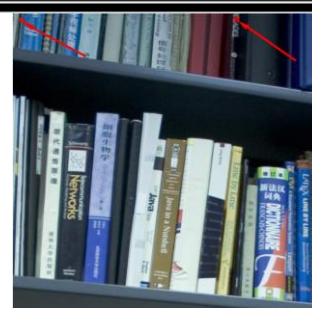
Розглянемо ЦЗ у вигляді сукупності непересічних блоків, отриманих стандартним чином, що очевидно відрізняються ступенем внеску високо/низькочастотної складової. Для наочності приклади таких зображень представлені на рис.1(а) - ЦЗ зі значними перепадами значень яскравості – велика кількість об'єктів різного розміру, порівняно значний вміст високочастотної складової, на рис.2(а) – ЦЗ, що має велику частину з незначними перепадами значень яскравості, незначну кількість об'єктів, ліній контурів на зображенні, порівняно значний вміст низькочастотної складової. З отриманого вище випливає, що для другого (далі – «фонового») зображення кількість блоків, де $svdgap_n(1) \approx 1$, буде значно більше, ніж для першого (далі – «контурного»), крім цього, для першого може бути значна кількість блоків, які містять малі деталі, контури, мають значні перепади значень яскравості пікселів, тобто де $svdgap_n(1) << 1$. Всі ці передбачення в сукупності підтверджуються конкретними властивостями гістограм $svdgap_n(1)$ для цих ЦЗ, які очікувано відрізняються. Позначимо Γ_F і Γ_K - гістограми $svdgap_n(1)$ для фонового і контурного ЦЗ відповідно.

Відмінності у властивостях Γ_F і Γ_K обумовлені ступенем відносного внеску високо/низькочастотної складової в блок ЦЗ і, враховуючи, що переважна кількість блоків фонового зображення має СНЧ $\sigma_2(B),..., \sigma_l(B)$, значення яких порівняні з нулем, а $svdgap_n(1)$ порівняну з одиницею, є наступними:

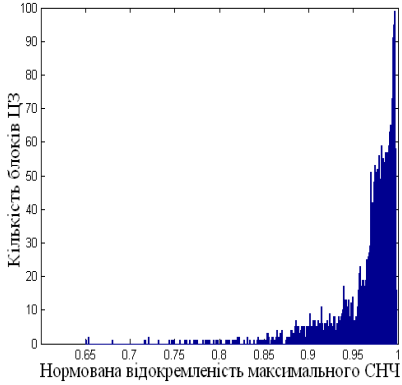
- Моди $m(\Gamma_F)$ і $m(\Gamma_K)$ гістограм Γ_F і Γ_K відповідають співвідношенню: $m(\Gamma_F) \geq m(\Gamma_K)$;
- значення в модах $V(m(\Gamma_F))$ і $V(m(\Gamma_K))$ відповідають співвідношенню: $V(m(\Gamma_F)) >> V(m(\Gamma_K))$.

При цьому незначному околу $m(\Gamma_F)$ відповідає, як правило, вклад переважної більшості блоків ЦЗ (аж до 95%), тоді як для контурного зображення поза таким околом, як правило, буде знаходитися вклад значної кількості блоків (понад 50%);

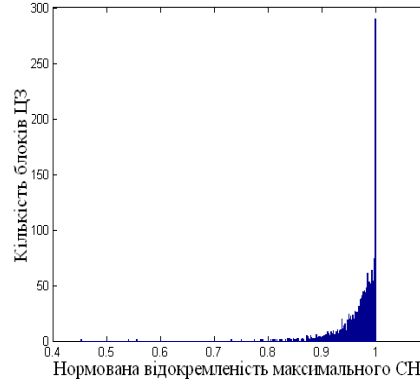
- В Γ_F розкид можливих значень $svdgap_n(1)$ не перевищує розкид в Γ_K, при цьому значення гістограми Γ_F в аргументах, що не належать малому околу моди, будуть порівняні з нулем.



а



б



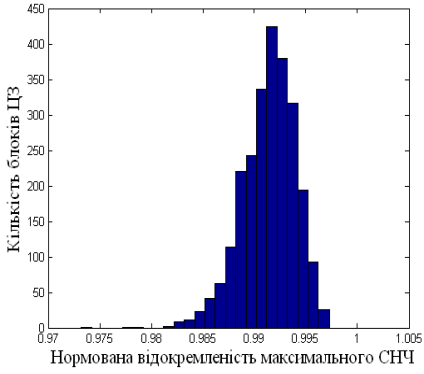
в

Рисунок 1. Гістограми значень НВМСЧ для конкретного «контурного» ЦЗ: а – оригінальне ЦЗ в форматі без втрат, б – Γ_K для оригінального ЦЗ; в - гістограма НВМСЧ для ЦЗ, перезбереженого у формат Jpeg (*QF*=75)

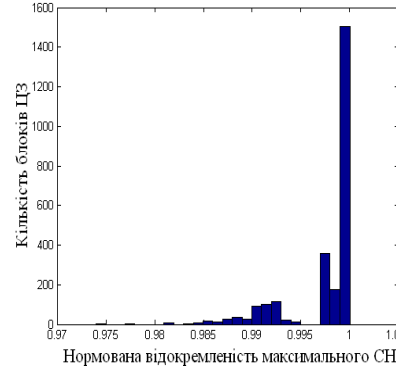
Відіб'ється на $svdgap_n(1)$ і процес зменшення високочастотної складової у блоках ЦЗ (незалежно від його первісного формату (з/без втрат)) в результаті відповідної обробки ЦЗ, такої як розмиття, збереження в форматі з втратами тощо: відбудеться «зсув» як Γ_F, так і Γ_K вправо, що є результатом незменшення $svdgap_n(1)$, який призведе до:

- незменшення значень $m(\Gamma_F)$ і $m(\Gamma_K)$; збільшення значень $V(m(\Gamma_F))$ і $V(m(\Gamma_K))$.

а



б



в

Рисунок 2. Гістограми значень НВМСЧ для конкретного «фонового» ЦЗ:
а – оригінальне ЦЗ в форматі без втрат, б – Γ_F для оригінального ЦЗ;
в - гістограма НВМСЧ для ЦЗ, перезбереженого у формат Jpeg (*QF*=75)

Отримані теоретичні висновки знайшли практичне підтвердження в ході обчислювального експерименту, типові результати якого продемонстровані на рис.1,2 у вигляді гістограм значень $svdgap_n(1)$ для блоків ЦЗ, що очевидно відрізняються відносним вмістом високочастотної/низькочастотної складової.

Все вищенаведене говорить на користь використання (5) як інтегрального параметра для оцінки вкладу високочастотної/низькочастотнох складової в блок ЦЗ і практично підтверджує перспективність підходу до вибору блоків для СПр, заснованого на аналізі $svdgap_n(1)$.

Метод вибору блоків зображення-контейнера для вбудови додаткової інформації

Як зазначено вище, для забезпечення потенційної можливості декодуваня ДІ після атаки проти вбудованого повідомлення величина збурення контейнера в результаті СПр повинна бути не менше, ніж величина збурення СП в результаті атаки, наслідком чого є більш значні збурення контейнера під час СПр за допомогою методу, стійкого до значних ЗД, а тому і забезпечення тут надійності сприйняття є більш складною задачею в порівнянні з аналогічною вимогою для метода, що не забезпечує стійкість. Яскравим прикладом тут може слугувати метод Коха і Жао, ступінь стійкості якого до атак протии вбудованого повідомлення залежить від вибори конкретних коефіцієнтів дискретного косинусного перетворення (ДКП) блоку, які задіюються в процесі вбудови ДІ [1] – стійкість буде зростати зі зменшенням частоти, коефіцієнти якої змінюються певним чином при СПр. При цьому при зменшенні частоти використовуваних коефіцієнтів ДКП при СПр буде збільшуватися ступінь спотворення контейнера і зменшуватися ймовірність збереження надійності сприйняття СП (рис.3).

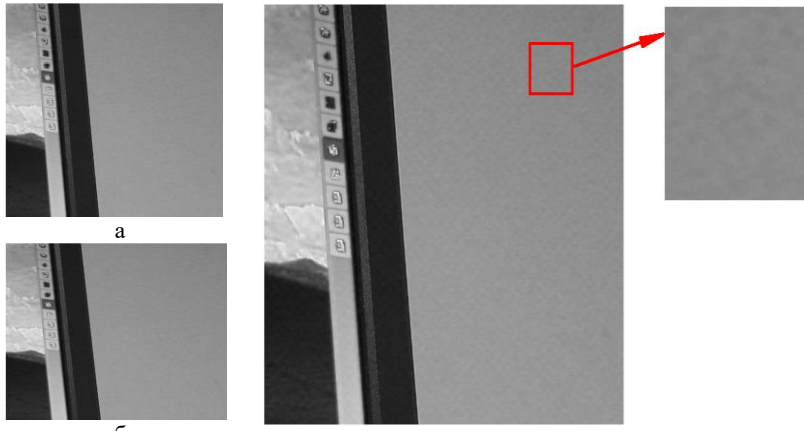


Рисунок 3. Ілюстрація візуальної якості СП, отриманого методом Коха і Жао при розбивці матриці контейнера на 8×8-блоки і задіюванні всіх блоків для СПр: а – оригінальне ЦЗ-контейнер; б – СП, отримане з використанням (4,5) и (5,4) коефіцієнтів ДКП; в - СП, отримане з використанням (2,3) и (3,2) коефіцієнтів ДКП

Ймовірність збереження надійності сприйняття (блоку) спотвореного ЦЗ, враховуючи особливості людської зорової системи [7] зростає, якщо це зображення (блок) містить маленькі деталі, значну кількість контурів, тобто має значну високочастотну складову. Таким чином, для забезпечення можливості застосування довільного, зокрема стійкого до атак проти вбудованого повідомлення, стеганоалгоритма до випадкового контейнера має

сенс задіювати в процесі СПр блоки контейнера зі значною високочастотною складовою, тобто такі, які мають відносно велике значення $svdgap_n(1)$.

Таким чином, основні кроки методу вибору блоків ЦЗ-контейнера для підвищення ймовірності забезпечення надійності сприйняття СП, в тому числі отриманого за допомогою стійкого до атак проти вбудованого повідомлення стеганографічного методу, який далі називається *SelectBlock*, наступні.

Крок 1. Матрицю F ЦЗ-контейнера розміром $n \times n$ розбити стандартним чином на непересічні $l \times l$-блоки $B_{ij}, i, j = \overline{1, \lceil n/l \rceil}$. Розрахувати t – кількість блоків контейнера, необхідну для вбудови ДІ, що є результатом попереднього кодування і представляє цифрову, як правило, бінарну, послідовність: $p_1, p_2, \ldots, p_m$.

Крок 2. Для кожного блоку $B_{ij}, i, j = \overline{1, \lceil n/l \rceil}$:

2.1. Обчислити СНЧ (за допомогою сингулярного розкладання (1)), визначити вектор сингулярного спектру: $\sigma = (\sigma_1(B_{ij}), \sigma_2(B_{ij}), \ldots, \sigma_l(B_{ij}))^T$;

2.2. Визначити нормований вектор сингулярного спектру блоку: $\overline{\sigma} = \sigma / \|\sigma\|$;

2.3. Знайти НВМСЧ блоку $svdgap_n(1)$ (5).

Крок 3. Впорядкувати блоки $B_{ij}, i, j = \overline{1, \lceil n/l \rceil}$ за неспаданням $svdgap_n(1)$. Перші t з них – блоки, що рекомендовані для вбудови ДІ.

Очевидно, що застосування запропонованого методу має сенс проводити лише тоді, коли $t < \lceil n/l \rceil$, тобто, коли є можливість використовувати не всі блоки контейнеру для пересилання наявного секретного повідомлення. Більше того, очікувати значний ефект можна тоді, коли $t << \lceil n/l \rceil$, і тут: чим більше t відрізняється від $\lceil n/l \rceil$, тим більше «поле вибору», тим кращий результат в сенсі забезпечення надійності сприйняття СП можна очікувати. Як показує практика, метод має сенс застосовувати, коли

$$t < \lceil n/l \rceil / 2. \quad (6)$$

Якщо (6) для ЦЗ не виконується, для пересилання наявного секретного повідомлення можна застосовувати у якості контейнера не одне, а декілька ЦЗ (чи цифрове відео, кадри якого розглядаються як ЦЗ), для кожного з яких умова (6) буде мати місце.

Запропонований метод *SelectBlock* є блоковим, що визначає його обчислювальну складність для $n \times n$-ЦЗ як $\underline{O}(n^2)$, але це не обмежує область його застосування тільки блоковими стеганографічними методами: він може бути використаний і для стеганометодів, що не є блоковими, наприклад, для (різноманітних модифікацій) методу модифікації найменшого значущого біта [22], виділяючи в ЦЗ-контейнері його області у вигляді об'єднання блоків, найбільш сприятливі для вбудови ДІ.

Тестування запропонованого методу *SelectBlock* проводилося з використанням множини з 800 ЦЗ розміром 800×800 пікселів з баз [23,24]. В кожне з цих ЦЗ, які розбивалися на непересічні 8×8-блоки (загальна кількість блоків – 10000) вбудовувалася ДІ – сформована випадковим чином бінарна послідовність довжини $t = 3500$, яка протягом всього експерименту залишалася незмінною. Вбудова ДІ проводилася двома стеганографічними методами: Коха і Жао [1] і методом, запропонованим в [4], що на сьогодні залишається одним з найстійкіших до атаки стиском. Для кожного ЦЗ-контейнера СПр кожним з методів проводилося двічі: блоки для вбудови ДІ обиралися довільним (випадковим) чином; блоки обиралися у відповідності з рекомендаціями, що надає *SelectBlock.* В кожному разі обчислювалася кількісна оцінка спотворення ЦЗ-контейнера – *PSNR*. Результати, які надають безумовну перевагу над довільним вибором блоку методу *SelectBlock,* наведені в табл..1. Зафіксоване підвищення значення *PSNR* на 8.39% для методу Коха і Жао, і на 7.13% для методу [4].

Таблиця 1

Середнє значення *PSNR* в результаті вбудови ДІ

Стеганометод	Середнє значення *PSNR* (dB)	
	Вибір блоків випадковим чином	Вибір блоків з використанням рекомендацій *SelectBlock*
Коха і Жао	42.54	46.11
Метод [4]	41.23	44.17

Метод визначення цифрових зображень, небажаних для використання в якості стеганографічних контейнерів

Запропонований підхід, заснований на використанні НВМСЧ, може бути застосований для відкидання ЦЗ, які не бажано використовувати в якості контейнера – зображень, що мають значну частину з невеликими перепадами значень яскравості пікселів. І хоча це не забезпечує ефективну роботу стеганометоду з випадковим контейнером, а передбачає його вибір, але дає можливість підвищити ефективність наявних методів без їх модифікації. Виходячи з вищенаведеного, потрібні висновки можна зробити, аналізуючи в сукупності властивості блоків ЦЗ, тобто аналізуючи гістограму $svdgap_n(1)$ блоків.

Основні кроки методу, що використовується для «відкидання» небажаних для ролі контейнера ЦЗ і далі називається *SelectImage*, наступні.

Крок 1. Матрицю F ЦЗ розміром $n \times n$ розбити стандартним чином на непересічні $l \times l$-блоки $B_{ij}, i, j = \overline{1, \lfloor n/l \rfloor}$.

Крок 2. Співпадає з кроком 2 методу *SelectBlock.*

Крок 3. Побудувати гістограму Γ значень $svdgap_n(1)$ для блоків досліджуваного ЦЗ.

Крок 4. Визначити моду гістограми $m(\Gamma)$.

Крок 5. Визначити окіл $m(\Gamma)$ незначного радіусу δ : $[m(\Gamma)-\delta, m(\Gamma)+\delta]$, де δ - параметр, що визначається експериментально.

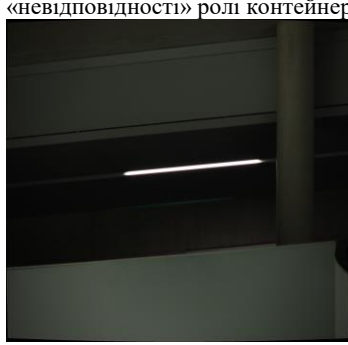
Крок 6. Розрахувати відносну кількість блоків ЦЗ (%) *W*, для яких $svdgap_n(1) \in [m(\Gamma)-\delta, m(\Gamma)+\delta]$.

Крок 7. *Якщо* $W > P$,

то досліджуване зображення не бажано використовувати як контейнер,

де *P* – порогове значення, встановлюване експериментально

Для алгоритмічної реалізації використовуються наступні значення параметрів: *l*=8, $\delta = 0.006$, *P*=86%. При проведенні обчислювального експерименту для оцінки ефективності *SelectBlock* використовувалися 1000 ЦЗ розміром 400×400 пікселів з баз зображень [23, 24, 25] – множина *M*. При застосуванні *SelectImage* з множити *M* було видалено 183 ЦЗ, приклади яких представлені на рис.4, які повністю відповідають суб'єктивній оцінці їх «невідповідності» ролі контейнера.



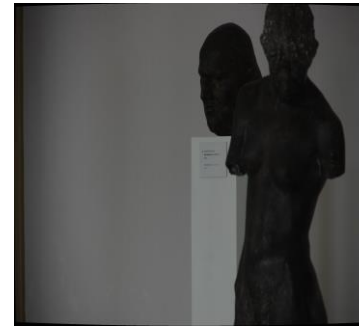


Рисунок 4. ЦЗ з бази [23], що були обрані як небажані для застосування в ролі контейнера методом *SelectImage*

Зображення, що залишилися, були об'єднані в множину $\overline{M}$. ЦЗ з множини *M* піддавалися СПр (вбудовувалася одна й та сама ДІ) методом Коха і Жао з використанням коефіцієнтів ДКП (4,5) і (5,4). Блоки та їх послідовність обиралися випадковим чином. Для кожного СП обраховувалося значення *PSNR*. При цьому середнє значення $PSNR_M$ для ЦЗ з множини *M* склало $PSNR_M = 36.41\,dB$, а по множині $\overline{M}$ - $PSNR_{\overline{M}} = 38.10\,dB$, що говорить про покращення (підвищення) на 4.64% кількісного показника спотворення ЦЗ при СПр в результаті застосування *SelectImage*. Звичайно, цей відсоток буде залежати від вмісту множини *M*: чим менше там первісно буде фонових ЦЗ, тим меншим буде відсоток збільшення $PSNR_M$, але при застосуванні *SelectImage* зменшення $PSNR_M$ не спостерігатиметься.

Обчислювальна складність *SelectImage* для ЦЗ з $n \times n$-матрицею, враховуючу його блокову організацію, визначається аналогічно обчислювальній складності *SelectBlock* і становить $\underline{O}\left(n^2\right)$ операцій.

Висновки

В роботі вирішена важлива науково-практична задача підвищення ефективності стеганосистеми при використанні довільного стеганометоду, в тому числі, стійкого до атак проти вбудованого повідомлення, який може призвести до значних спотворень контейнера, і випадкового контейнеру шляхом розробки методу вибору блоків ЦЗ-контейнера для вбудови в них ДІ, де ефективність стеганосистеми оцінювалась ступенем спотворення контейнера в результаті вбудови ДІ, який кількісно розраховувався за допомогою показника *PSNR* - пікового відношення «сигнал-шум».

В ході роботи отримані наступні результати:

- обґрунтовано вибір інтегрального показника розподілу частотних складових блоку ЦЗ (незалежно від формату збереження: з/без втрат) – нормованої відокремленості максимального СНЧ та досліджені його властивості, що дало можливість для побудови методу вибору блоків на основі кількісного аналізу $svdgap_n(1)$, який дозволив при своєму застосуванні підвищити ефективність стеганосистеми більше, ніж на 7% при використанні стеганометодів, що не гарантують системне забезпечення надійності сприйняття формованного СП;
- встановлені відмінності між гістограмами значень $svdgap_n(1)$ для ЦЗ, що відрізняються відносним вмістом низькочастотної/високочастотної складової, що дало можливість для побудови методу визначення небажаних для ролі контейнера ЦЗ – зображень зі значною областю з малими перепадами значень яскравості, що дало можливість підвищити ефективність стеганосистеми в сенсі забезпечення надійності сприйняття СП більше, ніж на 4%;
- обидва запропоновані методи мають незначну обчислювальну складність, яка для ЦЗ з $n \times n$-матрицею становить $\underline{O}\left(n^2\right)$ операцій. Така обчислювальна складність для методу вибору блоків в ЦЗ-контейнері забезпечує перспективу його використання для потокового контейнеру.

Література

1. Konakhovich, G. F., Progonov, D. O., & Puzirenko, O. Y. (2018). *Computer steganographic processing and analysis of multimedia data*. Kyiv, UA: Center for Educational Literature.

2. Karampidis, K., Kavallieratou, E., & Papadourakis, G. (2018). A review of image steganalysis techniques for digital forensics. *Journal of Information Security and Applications, 40,* 217–235. https://doi.org/10.1016/j.jisa.2018.04.005

3. Bohang, L., et al. (2025). Image steganalysis using active learning and hyperparameter optimization. *Scientific Reports, 15,* Article 7340. https://doi.org/10.1038/s41598-025-92082-w

4. Melnik, M. A. (2012). Compression-resistant steganography algorithm. *Information Security, 2,* 99–106.

5. Kozina, M. O. (2015). Method of verification of authenticity of information that is passed by steganographic communication channel. *Visnyk of Vinnytsia Polytechnical Institute, 1,* 117–121.

6. Michaylov, K. D., & Sarmah, D. K. (2024). Steganography and steganalysis for digital image enhanced forensic analysis and recommendations. *Journal of Cyber Security Technology, 9*(1), 1–27. https://doi.org/10.1080/23742917.2024.2304441

7. Gonzalez, R. C., & Woods, R. E. (2007). *Digital image processing* (3rd ed.). London, UK: Pearson.

8. Srinivasan, D., Manojkumar, K., Syed, A., & Nutakki, H. (2025). A comprehensive review on advancements and applications of steganography. *ResearchGate.* Retrieved June 1, 2025, from https://doi.org/10.13140/RG.2.2.13568.44807

9. Kobozeva, A. A., Machalin, I. O., & Khoroshko, V. O. (2010). *Security analysis of information systems*. Kyiv, UA: DUIKT.

10. Bergman, C., & Davidson, J. (2025). Unitary embedding for data hiding with the SVD. *Iowa State University of Science and Technology.* Retrieved June 1, 2025, from https://dr.lib.iastate.edu/handle/20.500.12876/54635

11. Kobozeva, A. A., & Sokolov, A. V. (2022). The sufficient condition for ensuring the reliability of perception of the steganographic message in the Walsh-Hadamard transform domain. *Problemele Energeticii Regionale, 2,* 84–100. https://doi.org/10.52254/1857-0070.2022.2-54.08

12. Pramanik, S., Ghonge, M. M., Ravi, R. V., & Cengiz, K. (Eds.). (2021). *Multidisciplinary approach to modern digital steganography*. Hershey, USA: IGI Global.

13. Abdulla, A. A. (2024). Digital image steganography: Challenges, investigation, and recommendation for the future direction. *Soft Computing, 28,* 8963–8976. https://doi.org/10.1007/s00500-023-09130-8

14. Rudnitsky, V. M., & Kostyrka, O. V. (2013). Robust steganotransformation in spatial domain of cover image. *Informatics and Mathematical Methods in Simulation, 3*(4), 353–360.

15. Kostyrka, O. V. (2016). Modification of resistance to disturbance quilted transformation of spatial image container. *Informatics and Mathematical Methods in Simulation, 6*(1), 85–93.

16. Qiao, T., et al. (2023). Robust steganography in practical communication: A comparative study. *EURASIP Journal on Image and Video Processing, 2023,* Article 15. https://doi.org/10.1186/s13640-023-00615-y

17. Liu, Q., et al. (2022). A robust image steganographic scheme against general scaling attacks. *arXiv.* arXiv:2212.02822

18. Bobok, I. I. (2018). Steganalysis method for detection of the hidden communication channel with low capacity. *Telecommunications and Radio Engineering*, *77*(18), 1597–1604. https://doi.org/10.1615/TelecomRadEng.v77.i18.20

19. Bobok, I., Kobozieva, A., & Kushnirenko, N. (2021). Use of the normalized gap of maximum singular value of the image block to evaluate the capacity of the steganographic channel. In *Proceedings of the 3rd International Conference on Information Security and Information Technologies (ISecIT 2021)* (pp. 183–188).

20. Kobozeva, A. A., Bobok, I. I., & Kushnirenko, N. I. (2022). Method for distinguishing the digital images in different formats. *Problemele Energeticii Regionale, 1,* 109–124. https://doi.org/10.52254/1857-0070.2022.1-53.09

21. Demmel, J. W. (1996). *Applied numerical linear algebra*. Philadelphia, USA: SIAM.

22. Aslam, M. A., et al. (2022). Image steganography using least significant bit (LSB) – A systematic literature review. In *Proceedings of the 2022 2nd International Conference on Computing and Information Technology (ICCIT)* (pp. 32–38). https://doi.org/10.1109/ICCIT52419.2022.9711628

23. Gloe, T., & Böhme, R. (2010). The Dresden Image Database for benchmarking digital image forensics. In *Proceedings of the 2010 ACM Symposium on Applied Computing (SAC '10)* (pp. 1584–1590). https://doi.org/10.1145/1774088.1774427

24. NRCS Photo Gallery. (2025). *USDA.* Retrieved June 1, 2025, from https://www.nrcs.usda.gov

25. Hsu, Y.-F., & Chang, S.-F. (2006). Detecting image splicing using geometry invariants and camera characteristics consistency. In *Proceedings of the 2006 IEEE International Conference on Multimedia and Expo* (pp. 549–552). https://doi.org/10.1109/ICME.2006.262447

NORMALIZED SEPARABILITY OF THE MAXIMUM SINGULAR NUMBER OF A DIGITAL IMAGE BLOCK AS AN INDICATOR OF THE FEASIBILITY OF ITS STEGANOTRANSFORMATION

Dr.Sci. I. Bobok[1][0000-0003-4548-0709], **Dr.Sci. A. Kobozova**[2][https://orcid.org/0000-0001-7888-0499]

[1]Odesa Polytechnic National University, Ukraine,
[2]Odesa National Maritime University, Ukraine
EMAIL: [1]onu_metal@ukr.net, [2]alla_kobozeva@ukr.net

Abstract. *One of the most promising and effective directions in information security today is steganography. Among a number of requirements for a steganographic system, one of the key ones is ensuring the reliability of perception of the steganogram. However, many existing steganographic methods, particularly those robust against attacks on the embedded message, are unable to systematically*

ensure this requirement and are not designed to work with a random container, which is most frequently used in practice. The aim of this work is to increase the efficiency of a steganographic system when using an arbitrary steganographic method and a random container. This is achieved through the development of a method for selecting container blocks from a digital image to embed additional information within them. The criterion for efficiency is the reliability of perception of the generated steganogram, quantitatively evaluated using PSNR. The goal was achieved by investigating the properties of formal parameters of digital image blocks – singular values, considering the correspondence between singular triplets and the frequency components of the block. The most important result of this work is the theoretically substantiated definition of a block parameter that provides an integral quantitative characteristic of the relative distribution of its frequency components – the normalized separability of the maximum singular value of the block. The practical significance of the obtained results lies in the development of a method for selecting image blocks and a method for identifying images undesirable for use as containers. The algorithmic implementations of these methods have significantly improved the efficiency of the steganographic system when applied.

***Keywords**: steganography, digital image, reliability of perception of the steganogram, container block selection, container selection, normalized separability of the singular value*

UDC 004.623
DOI https://doi.org/10.36059/978-966-397-538-2-5

ІНТЕЛЕКТУАЛЬНИЙ ГІБРИДНИЙ ПРОЄКТ СИСТЕМИ ДЛЯ АНАЛІЗУ РИЗИКІВ ШКОДИ ЗДОРОВ'Ю ПРИ ВЕЛИКИХ ОБСЯГАХ ДАНИХ

Ph.D. М. Рудніченко[1][0000-0002-7343-8076], **Ph.D. Н. Шибаєва**[1][0000-0002-7869-9953], **Ph.D. Т. Отрадська**[2][0000-0002-5808-5647], **Д. Шведов**[1][0009-0002-4823-8782], **Ph.D. І. Шпінарева**[1][0000-0001-9208-4923], **Dr.Sci. І.Петров**[1][0000-0002-8740-6198]

[1]Національний університет «Одеська Політехніка», Україна,
[2]Одеський коледж комп'ютерних технологій «СЕРВЕР», Україна
EMAIL: nickolay.rud@gmail.com, nati.sh@gmail.com, tv_61@ukr.net, frumle@ukr.net, iryna.shpinareva@onu.edu.ua, firmn@gmail.com

***Анотація.** У статті представлено всебічне дослідження щодо розробки проекту гібридної інтелектуальної системи для аналізу ризиків шкоди здоров'ю населення на великих обсягах екологічних даних, спричиненої забрудненням повітря, із використанням гібридної архітектури на основі моделей машинного та глибинного навчання. Актуальність дослідження обґрунтована зростаючими загрозами для здоров'я, пов'язаними з атмосферними забруднювачами, такими як PM2.5, PM10, NO_2, SO_2, CO та*