DOI: https://doi.org/10.17721/ISTS.2020.1.16-22
УДК 004.056.5

РОЗРОБКА СТЕГАНОГРАФІЧНОГО МЕТОДУ, СТІЙКОГО ДО АТАК ПРОТИ ВБУДОВАНОГО ПОВІДОМЛЕННЯ

Кобозєва Алла
orcid.org/0000-0001-7888-0499

Бобок Іван
orcid.org/0000-0003-4548-0709

м. Одеса, Одеський національний політехнічний університет, alla_kobozeva@ukr.net
м. Одеса, Одеський національний політехнічний університет, onu_metal@ukr.net

Історія статті:
Надійшла до редакції 15.01.2020
Прийнято 22.01.2020

Ключові слова:
стеганографічний метод;
цифрове зображення;
стійкість до атак;
сингулярне число;
блок матриці

Анотація. Особливості сучасних мережевих комунікацій приводять до необхідності використання при організації прихованого каналу зв'язку стеганографічних алгоритмів, стійких до стиску з втратами, залишаючи актуальними задачі розробки нових ефективних стеганометодів. В роботі на основі загального підходу до аналізу стану й технології функціонування інформаційних систем, який базується на теорії збурень та матричного аналізу, розроблено новий блоковий поліноміальний ступеня 2 стеганографічний метод, стійкий до атак проти вбудованого повідомлення, в тому числі значних, з одночасним збереженням надійності сприйняття формованого стеганоповідомлення, що забезпечується використаним математичним базисом. В якості контейнера розглядається цифрове зображення. Пропускна спроможність прихованого каналу зв'язку, що будується за допомогою розробленого методу, дорівнює n^{-2} біт/піксель при будь-якій алгоритмічній реалізації за умови використання всіх $n\times n$-блоків матриці контейнера, отриманих в результаті стандартної розбивки його матриці, при стеганоперетворенні. Вбудова додаткової інформації, що представляє бінарну послідовність і є результатом попереднього кодування інформації, що приховується, робиться шляхом використання нечутливих до збурних дій формальних параметрів матриці контейнера – сингулярних чисел її блоків малого розміру ($n\leq 8$). Забезпечення стійкості методу до збурних дій та надійності сприйняття формованого стеганоповідомлення досягається шляхом збільшення максимального сингулярного числа блоку, задіяного в стеганоперетворенні, при цьому величина збільшення визначається з використанням значень, отриманих шляхом піднесення сингулярних чисел блоку у натуральний ступінь k. Алгоритмічна реалізація методу вимагає додаткових досліджень для встановлення залежності значення параметру k від властивостей зображення-контейнеру.

Abstract. Features of modern network communications make it necessary to use in the organization of the hidden channel communication of steganographic algorithms that are resistant to loss compression, and leaving the tasks of developing new effective steganographic methods are relevant. The paper develops a new block steganographic method, which is resistant to attacks against the built-in message, including strong attacks. This method preserves the reliability of the perception of the formed quilting due to the mathematical basis used. It is based on a general approach to the analysis of the state and technology of information systems functioning, matrix analysis, perturbation theory. A digital image is treated as a container. The bandwidth of a hidden link that is built using the developed method is equal to n^{-2} bpp, $n\times n$ is the size of the blocks of the container that are obtained by the standard breakdown of its matrix. Such bandwidth is achieved with any algorithmic implementation of the method. Additional information is a binary sequence, it is the result of pre-coding of the information that is hidden. The embedding of additional information is done by using formal container matrix parameters that are insensitive to perturbation. These are singular values of its small blocks ($n\leq 8$). Increasing the maximum singular value of the block, which occurs when embedding additional information, leads to the stability of the method to the perturbing action and to ensure the reliability of the perception of the hip. The magnitude of the increase in the maximum singular value is determined using the values obtained by

raising the singular values of the block to a natural degree *k*. Algorithmic implementation of the method requires additional studies to determine the parameter *k*.

1. ВСТУП

На сьогоднішній день одною з важливих складових комплексного захисту інформації є стеганографічний захист [1-3]. У сучасному інформаційному суспільстві дослідження й розробки в області стеганографії стають усе більш популярними, і для цього є декілька причин:

- зростання актуальності проблеми захисту прав власності на інформацію, яка представлена в цифровому виді, у зв'язку з неперервним зростанням її цінності;
- обмеження на використання крипто-засобів у ряді країн світу, у тому числі, в Україні;
- для розв'язку задач інформаційної безпеки часто недостатньо зробити інформацію недоступною для порушника, потрібно приховати сам факт її передачі або зберігання.

В процесі стеганографування інформація, яка приховується, піддається попередньому кодуванню, в результаті якого отримується, як правило, бінарна послідовність, що далі називається додатковою інформацією (ДІ), яка вбудовується в деякий інформаційний контент – контейнер, що не привертає уваги, в результаті чого отримується стеганоповідомлення [3]. Стеганоповідомлення може передаватися каналами загального користування або зберігатися в отриманому вигляді. На сьогодні найчастіше як контейнери використовуються цифрові зображення (ЦЗ), які далі розглядаються в роботі.

Особливості сучасної комунікації, стрімке зростання обсягів інформації, що передається по каналах зв’язку, приводять до необхідності використання при організації прихованого каналу зв’язку стеганографічних алгоритмів, стійких до атак проти вбудованого повідомлення [3], зокрема до стиску з втратами. І хоча для стеганоперетворення можуть використовуватися як просторова область ЦЗ-контейнера, так і область перетворення [4,5], при організації стеганографування, коли мова йде про стійкість розроблюваних методів до атак, використовуються, як правило, області перетворення ЦЗ: частотна, області різних розкладань матриці (матриць) ЦЗ-контейнера. Розробці таких стеганоалгоритмів присвячено багато зусиль сучасних фахівців в галузі інформаційної безпеки [6-10], але, враховуючи можливу критичну важливість обсягу правильно відновленої інформації при організації прихованого каналу зв’язку в різних умовах його використання, зокрема, в умовах значних збурних дій (ЗД), питання підвищення ефективності таких алгоритмів залишається *актуальним*.

2. МАТЕРІАЛИ І МЕТОДИ

Існування значної кількості стійких до атак проти вбудованого повідомлення стеганографічних методів ще нещодавно ніяк не забезпечувалося наявністю математичних достатніх умов такої стійкості. Більшість з таких алгоритмів була розрахована на конкретні атаки, враховуючи їх специфіку, при цьому, хоча деякі з існуючих стеганографічних методів і позиціонувалися як стійкі до атак, незалежно від їх природи (та сили), але на практиці, в силу відсутності «універсального» математичного базису, їх реалізації все одно були розраховані на конкретні збурні дії (частіше, незначні) [11-14]. Більше того, деякі з фахівців-науковців обгрунтовано відкидали саму можливість створення таких методів. Наприклад, автори [15] стверджують, що стеганоалгоритм може бути стійким до стиску ЦЗ тільки тоді, коли він буде враховувати особливості алгоритму перспективного стиску, тобто алгоритм, стійкий до стиску, заснованому на вейвлет-перетворенні (JPEG2000), не може бути стійким до стиску, заснованому на дискретному косинусному перетворенні (JPEG). З урахуванням того, що стиск є лише одною з ЗД на стеганоповідомлення, специфікою якої є обнуління високочастотних складових сигналу, така думка обмежує можливості для побудови універсальних стеганоалгоритмів, стійких до атак проти вбудованого повідомлення, відволікаючи авторів розробок на врахування специфіки збурної дії.

В [16,17] вперше були запропоновані формальні умови забезпечення стійкості стеганоалгоритму до атак проти вбудованого повідомлення на основі загального підходу до аналізу стану й технології функціонування інформаційних систем [17]. Саме на основі цих достатніх умов в [8, 18] були запропоновані ефективні стеганографічні методи, алгоритмічні реалізації яких є стійкими до атак, зокрема значних, що використовують область сингулярного розкладання відповідної матриці [19], засновані на залученні до стегано-перетворення сингулярних чисел (СНЧ) [18] та сингулярних векторів (СНВ) [8] блоків матриці ЦЗ-контейнера, отриманих шляхом стандартної розбивки [20], ефективність яких в умовах значних ЗД перевищує ефективність сучасних

аналогів завдяки використаному математичному апарату. Однак для запропонованих методів, як і для більшості існуючих стеганометодів, стійких в умовах значних збурних дій, можливим є порушення надійності сприйняття стеганоповідомлення [3, 21], що є значним недоліком при організації прихованого каналу зв'язку.

3. МЕТА СТАТТІ ТА ПОСТАНОВКА ЗАДАЧ ДОСЛІДЖЕННЯ

Враховуючи спроможність та унікальність для забезпечення стійкості стеганометодів до атак проти вбудованого повідомлення математичного базису, запропонованого в [16,17], заснованого на теорії збурень та матричному аналізі, який вже добре зарекомендував себе в області стеганографії, здається доцільним його застосування для розробок нових стійких стеганометодів та алгоритмів.

Метою роботи є розробка нового стеганографічного методу, стійкого до атак проти вбудованого повідомлення, в тому числі значних, з одночасним збереженням надійності сприйняття формованого стеганоповідомлення і забезпеченням прийнятної пропускної спроможності прихованого каналу зв'язку.

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

1. Вибір формальних параметрів матриці ЦЗ-контейнера, нечутливих до збурних дій, які доцільно використовувати для організації процесу стійкого стеганоперетворення;
2. Збільшення нечутливості обраних формальних параметрів до збурних дій шляхом їх обґрунтованого перетворення;
3. Забезпечення надійності сприйняття формованного стеганоповідомлення.

4. ОСНОВНА ЧАСТИНА

Для простоти викладу наступного матеріалу, не обмежуючи спільності міркувань, як формальне представлення ЦЗ розглядається одна двовимірна матриця *F*, яка піддається стандартній розбивці на *n*×*n*-блоки, довільний з яких далі позначається *B*. Оскільки стан (зміна стану) будь-якої інформаційної системи згідно з загальним підходом до аналізу стану й технології функціонування інформаційних систем формально може бути представлений у вигляді сукупності збурень СНЧ і СНВ відповідної матриці (блоків матриці) [17], а процес стеганоперетворення ЦЗ-контейнера є процесом збурення зображення, розглянемо сукупність СНЧ і СНВ *B*, побудувавши для нього нормальне сингулярне розкладання [22]:

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

де U, V – ортогональні $n\times n$-матриці лівих лексикографічно додатних і правих СНВ B відповідно, які представлені стовпцями u_i матриці U і v_i матриці V, $i = 1\ldots n$, $\Sigma = diag(\sigma_1,...,\sigma_n)$ - діагональна матриця СНЧ, $\sigma_1 \geq \ldots \sigma_n \geq 0$. Якщо СНЧ попарно різні, то розкладання (1) визначається однозначно [22]. СНЧ матриці (блоку матриці) ЦЗ є добре обумовленими, або нечутливими до збурних дій [19], чого не можна в загальному випадку сказати про СНВ [19], тому саме СНЧ розглядаються далі як формальні параметри ЦЗ-контейнера, які доцільно використовувати для організації процесу стеганоперетворення шляхом їх збурень. Відповідні СНЧ різних блоків навіть одного ЦЗ можуть значно відрізнятися одне від одного. Це ускладнює процес організації і аналізу їх збурень в процесі стеганоперетворення чи іншої збурної дії на стеганоповідомлення. Для полегшення цих процесів має сенс розглядати не самі СНЧ (в вигляді вектору $\sigma = (\sigma_1,\sigma_2,...,\sigma_n)^T$), а нормовані СНЧ, отримані шляхом нормування σ, результатом чого є вектор $\bar{\sigma} = \frac{\sigma}{\|\sigma\|}$, $\bar{\sigma} = (\bar{\sigma}_1,\bar{\sigma}_2,...,\bar{\sigma}_n)^T$, де $\|\sigma\|$ - норма вектора σ.

Для більшості блоків оригінального ЦЗ має місце співвідношення [17]:

$$\sigma_1 >> \sigma_2 \geq ... \geq \sigma_n \geq 0. \quad (2)$$

Враховуючи (2), в [23] отримано, що для таких блоків:

$$\angle(e_1,\bar{\sigma}) \approx 0, \quad (3)$$

де $\angle(e_1,\bar{\sigma})$ - кут між векторами $\bar{\sigma}$ і $e_1 = (1,0,...0) \in R^n$ - першим вектором стандартного базису простору R^n.

Оскільки вектор σ є стійким до збурних дій незалежно від природи і виду цієї дії, то такі ж властивості притаманні і вектору $\bar{\sigma}$.

Враховуючи, що для блоків оригінального ЦЗ в більшості з них точна рівність

$$\sigma_2 = ... = \sigma_n = 0 \quad (4)$$

не виконується, тобто в точності рівність (3) не досягається, то процес вбудови ДІ (біта ДІ) можна реалізувати шляхом збільшення в блоці,

що використовується при стеганоперетворенні, σ_1 на $\Delta > 0$ так, щоб в порівнянні з $\sigma_1 + \Delta$ всі інші СНЧ $\sigma_2,...,\sigma_n$ були такими, ненульовими значеннями яких можна було б знехтувати в умовах задачі, що розглядається, а кут $\angle\left(e_1,\bar{\sigma}\right)$, де вектор $\bar{\sigma}$ відповідає збільшеному першому СНЧ блоку ($\sigma_1 + \Delta$), практично дорівнював 0. Дійсно, оскільки

$$\left(e_1,\bar{\sigma}\right) = \|e_1\|\left\|\bar{\sigma}\right\| cos\left(\angle\left(e_1,\bar{\sigma}\right)\right) = cos\left(\angle\left(e_1,\bar{\sigma}\right)\right) = \\ = \frac{\sigma_1 + \Delta}{\sqrt{\left(\sigma_1 + \Delta\right)^2 + {\sigma_2}^2 + ... + {\sigma_n}^2}}, \quad (5)$$

де $(\cdot,\cdot)$ - скалярний добуток векторів-аргументів, в якості векторної норми для визначеності розглядається евклідова, то

$$\angle\left(e_1,\bar{\sigma}\right) = \arccos\frac{\sigma_1 + \Delta}{\sqrt{\left(\sigma_1 + \Delta\right)^2 + {\sigma_2}^2 + ... + {\sigma_n}^2}}. \quad (6)$$

Зрозуміло, що

$$\angle\left(e_1,\bar{\sigma}\right) \underset{\Delta\to\infty}{\to} 0, \quad (7)$$

але будь-які зміни СНЧ збурять матрицю ЦЗ. Враховуючи те, що для збереження надійності сприйняття стеганоповідомлення збурення матриці контейнера при стеганоперетворенні повинно бути незначним (чим менше збурення контейнера, тим більша ймовірність збереження надійності сприйняття стеганоповідомлення [17]), збурення блоку $\Delta > 0$ повинно бути якнайменше, щоб досягти такої близькості в (3), яка влаштує в умовах організації процесу стеганоперетворення. Таким чином, значення $\angle\left(e_1,\bar{\sigma}\right)$ хоча і повинно прямувати до нуля, але не за рахунок того, що $\Delta \to \infty$. З огляду на це розглянемо можливість застосування запропонованої ідеї зменшення кута $\angle\left(e_1,\bar{\sigma}\right)$, але не безпосередньо для вектору $\sigma = \left(\sigma_1,\sigma_2,...,\sigma_n\right)^T$, а для його перетворення.

В [24] доведено, що

$$\angle\left(e_1,\bar{\bar{\sigma}}\right) < \angle\left(e_1,\bar{\sigma}\right), \quad (8)$$

де $\bar{\bar{\sigma}} = \frac{\left({\sigma_1}^2,{\sigma_2}^2,...,{\sigma_n}^2\right)^T}{\left\|\left({\sigma_1}^2,{\sigma_2}^2,...,{\sigma_n}^2\right)^T\right\|} = \left(\bar{\bar{\sigma}}_1,\bar{\bar{\sigma}}_2,...,\bar{\bar{\sigma}}_n\right)^T$, $\angle\left(e_1,\bar{\bar{\sigma}}\right)$ - кут між векторами $\bar{\bar{\sigma}}$ і e_1, при цьому вектор $\bar{\bar{\sigma}}$ має меншу чутливість до збурних дій, ніж $\bar{\sigma}$, що принципово дає йому перевагу в порівнянні з $\bar{\sigma}$ в випадку залучення його до процесу стеганоперетворення, яке повинно бути стійким до атак проти вбудованого повідомлення.

Ступінь близькості будь-якого нормованого вектора, елементи якого задовольняють (2), до e_1 визначається відстанню між першою і другою компонентами (відповідно з (6), (7) для вектора СНЧ): чим більше ця відстань, тим ближче нормований вектор до e_1. Нехай СНЧ σ_1 збільшили на деяку величину Δ, тоді відстань $d = \sigma_1 - \sigma_2$ між σ_1 і σ_2 збільшиться на Δ і буде дорівнювати: $\bar{d} = d + \Delta$. В той же час відстань між ${\sigma_1}^2$ і ${\sigma_2}^2$ теж зміниться і буде дорівнювати:

$$\left(\sigma_1 + \Delta\right)^2 - {\sigma_2}^2 = \bar{d}\left(\sigma_1 + \sigma_2 + \Delta\right). \quad (9)$$

З врахуванням (2) і того, що $\Delta > 0$, з (9) випливає, що відстань між ${\sigma_1}^2$ і ${\sigma_2}^2$ збільшиться більше ніж між σ_1 і σ_2, що приведе до того, що після збурення σ_1 на $\Delta > 0$ відповідний збурений вектор $\bar{\bar{\sigma}}$ буде ближче до e_1, чим збурений вектор $\bar{\sigma}$; чи інакше: для того, щоб досягти однакової близькості з e_1 векторам $\bar{\sigma}$ і $\bar{\bar{\sigma}}$, першу компоненту вектору $\left({\sigma_1}^2,{\sigma_2}^2,...,{\sigma_n}^2\right)^T$ треба збільшити менше, ніж першу компоненту $\sigma = \left(\sigma_1,\sigma_2,...,\sigma_n\right)^T$. Це означає, що для організації стеганоперетворення за рахунок наближення вектора СНЧ (перетворених СНЧ) до вектора e_1 з більшою ймовірністю надійність сприйняття буде зберігатися у випадку вектора $\left({\sigma_1}^2,{\sigma_2}^2,...,{\sigma_n}^2\right)^T$.

Ефект (8), (9) (зростання відстані між першою та другою компонентами відповідного вектора) збільшиться ще більше, якщо розглянути вектор, елементами якого є СНЧ в ступені, більшому за 2: $\left({\sigma_1}^k,{\sigma_2}^k,...,{\sigma_n}^k\right)^T$. Взагалі, чим більше буде ступінь, тим до більшого збільшення відстані

між першим і другим елементом будемо приходити при збільшенні σ_1:

$$\left(\sigma_1+\Delta\right)^k-{\sigma_2}^k=\overline{d}\sum_{i=1}^{k}\left(\sigma_1+\Delta\right)^{k-i}{\sigma_2}^{i-1}. \quad (10)$$

тобто зменшення кута $\angle\left(e_1,\overline{\sigma}\right)$ до нуля (до значення, порівнянного з нулем) можна забезпечити не тільки за рахунок $\Delta\to\infty$ (7), що приведе до порушення надійності сприйняття стеганоповідомлення, а за рахунок збільшення ступеня СНЧ блоку ${\sigma_i}^k, i=\overline{1,n}$, при безпосередньому стеганоперетворенні при фіксованому (невеликому) значенні Δ:

$$\lim_{k\to\infty}\arccos\frac{\left(\sigma_1+\Delta\right)^k}{\sqrt{\left(\sigma_1+\Delta\right)^{2k}+{\sigma_2}^{2k}+\ldots+{\sigma_l}^{2k}}}=1. \quad (11)$$

З урахуванням (11) основні кроки метода, що пропонується, стійкого до атак, в тому числі, значних, проти вбудованого повідомлення, що зберігає надійність сприйняття стеганоповідомлення, наступні.

Вбудова ДІ

Крок 1. Матриця *F* ЦЗ-контейнера розбивається стандартним чином на $2l\times 2l$-блоки малого розміру ($n=2l$).

Крок 2. Черговий $2l\times 2l$-блок *B* контейнера, що використовується для вбудови 1 біта p_m ДІ і визначається згідно з секретним ключем, розбивається на чотири $l\times l$-блоки $B^{(i)}$, $i=\overline{1,4}$, що не перетинаються.

Крок 3. Для кожного з 4-х отриманих $l\times l$-блоків $B^{(i)}$, $i=\overline{1,4}$, знайти СНЧ $\sigma_1^{(i)}$ і $\sigma_2^{(i)}$ і відстані між їх *k*-ими ступенями: $d_k^{(i)}=\left(\sigma_1^{(i)}\right)^k-\left(\sigma_2^{(i)}\right)^k$. Обчислити $d_{max}=\max\limits_{1\le i\le 4}d_k^{(i)}$.

Крок 4. Згідно з секретним ключем залежно від значення p_m визначається конкретний блок $B^{(j)}$ в межах *B*, в який буде відбуватися безпосередньо вбудова p_m. В цьому блоці в результаті вбудови ДІ потрібно забезпечити

$$\left(\sigma_1^{(j)}\right)^k\ge\left(\sigma_2^{(j)}\right)^k+d_{max}+\Delta, \quad (12)$$

де $\Delta>0$. Це робиться шляхом збільшення СНЧ $\sigma_1^{(j)}$, результатом чого є $\sigma_{1,new}^{(j)}$:

$$\sigma_{1,new}^{(j)}\ge\sqrt[k]{\left(\sigma_2^{(j)}\right)^k+d_{max}+\Delta}. \quad (13)$$

Крок 5. Відновити $B_{new}^{(j)}$ з урахуванням нового значення першого СНЧ і незмінених інших СНЧ і СНВ.

Крок 6. Побудувати $2l\times 2l$-блок стеганоповідомлення, що відповідає блоку *B* контейнера, враховуючи незмінність всіх $B^{(i)}$, $i=\overline{1,4}, i\ne j$, і $B_{new}^{(j)}$.

Крок 7. Перехід на крок 2 до наступного блоку контейнера, задіяного в стеганоперетворенні, при наявності такого.

Крок 8. Закінчення формування стеганоповідомлення; результат – ЦЗ з матрицею $\overline{F}$.

Декодування ДІ

Крок 1. Матриця $\overline{F}$ ЦЗ-стеганоповідомлення розбивається стандартним чином на $2l\times 2l$-блоки.

Крок 2. Черговий $2l\times 2l$-блок $\overline{B}$ стеганоповідомлення, в якому міститься ДІ, що визначається згідно з секретним ключем, розбивається на чотири $l\times l$-блоки $\overline{B}^{(i)}$, $i=\overline{1,4}$, що не перетинаються.

Крок 3. Для кожного з 4-х отриманих $l\times l$-блоків $\overline{B}^{(i)}$, $i=\overline{1,4}$, знайти:

3.1. СНЧ: $\sigma_{1_S}^{(i)}$, $\sigma_{2_S}^{(i)}$,…, $\sigma_{l_S}^{(i)}$, $i=\overline{1,4}$;

3.2. Кути $\sigma_S^{(i)}$ між векторами $\left(\left(\sigma_{1_S}^{(i)}\right)^k,\left(\sigma_{2_S}^{(i)}\right)^k,\ldots,\left(\sigma_{l_S}^{(i)}\right)^k\right)^T$ і e_1, $i=\overline{1,4}$.

Крок 4. Визначити:

$$\sigma_S^{(j)}=\min_{1\le i\le 4}\sigma_S^{(i)}. \quad (14)$$

Декодування чергового біту $\overline{p}_m$ ДІ відбувається з $\overline{B}^{(j)}$. Значення $\overline{p}_m$ залежить від того, з якого саме $l\times l$-блоку $\overline{B}^{(j)}$ відбувається декодування (з врахуванням секретного ключа).

Крок 5. Перехід на крок 2 до наступного блоку стеганоповідомлення, задіяного в стеганоперетворенні, при наявності такого.

Крок 6. Закінчення декодування ДІ.

Зауваження 1. Враховуючу наявну кореляцію між значеннями сусідніх пікселів оригінального

ЦЗ, можна стверджувати, що значення $\sigma_1^{(i)}$, $i=\overline{1,4}$, не значно відрізняються одне від іншого [25], тому вибір конкретного блоку $B^{(j)}$ на кроці 4, який відбувається згідно з секретним ключем без врахування наступного спотворення блоку при стеганоперетворенні, не може привести до таких впливів на надійність сприйняття стеганоповідомлення, які будуть суттєво відрізнятися при різних значеннях *j*.

Зауваження 2. Головним при побудові алгоритмічної реалізації запропонованого методу є визначення параметру *k*. Це визначення повинно досягатися за допомогою компромісу між двома вимогами. По-перше, забезпечення близькості вектора $\left(\left(\sigma_{1,new}{}^{(j)}\right)^k,\left(\sigma_2{}^{(j)}\right)^k,...,\left(\sigma_n{}^{(j)}\right)^k\right)^T$ блоку $B_{new}{}^{(j)}$ до вектора e_1 при вбудові ДІ буде тим краще, чим більше буде значення *k*. Але, по-друге, при дуже великому *k* значення $\sigma_S^{(i)}$, $i=\overline{1,4}$, враховуючи особливості машинної арифметики, можуть практично не відрізнятися одне від одного, що може привести до помилок при визначенні блоку $\overline{B}^{(j)}$ для декодування чергового біта ДІ, тобто помилок при декодуванні.

Зауваження 3. Визначення параметру Δ, що використовується в процесі вбудови ДІ на 4 кроці, потребує аналізу спотворення ЦЗ в результаті стеганоперетворення. Параметр Δ повинен визначатися таким чином, щоб значення пікового відношення «сигнал-шум» (*PSNR*) для побудованого стеганоповідомлення було більшим за 35-40 dB, що вважається прийнятним при організації прихованого каналу зв'язку [15].

Зауваження 4. Запропонований метод є блоковим, тому його обчислювальна складність для ЦЗ розміром $t\times t$ визначається кількістю блоків, які не перетинаються, отриманих шляхом стандартної розбивки, тобто складає $\underline{O}\left(t^2\right)$ операцій.

Зауваження 5. При алгоритмічній реалізації запропонованого методу доцільно використовуватися блоки малого розміру: $n\leq 8$, оскільки для оригінальних ЦЗ співвідношення (4) при $n>8$ практично ніколи не виконується [25], а це означає, що його штучне досягнення в процесі вбудови ДІ в такому випадку може привести до порушення надійності сприйняття формованного стеганоповідомлення.

Зауваження 6. При вбудові ДІ на кроці 4 секретний ключ може визначати номер *j* блоку $B^{(j)}$ залежно від значення p_m, враховуючи, наприклад, його парність/непарність, тобто, якщо $p_m=0$, то $j=2\vee j=4$, інакше $j=1\vee j=3$. В такому випадку парність/непарність *j* для $\overline{B}^{(j)}$ на кроці 4 декодування визначить $\overline{p}_m$.

Пропускна спроможність прихованого каналу зв'язку, що будується за допомогою розробленого методу, буде дорівнювати n^{-2} біт/піксель при будь-якій алгоритмічній реалізації за умови використання всіх блоків матриці ЦЗ-контейнера, отриманих в результаті стандартної розбивки. Така пропускна спроможність є прийнятною для сучасних стеганометодів [15].

5. ВИСНОВКИ

В роботі на основі теорії збурень та матричного аналізу розроблено новий блоковий стеганографічний метод, стійкий до атак проти вбудованого повідомлення, в тому числі значних, з одночасним збереженням надійності сприйняття формованого стеганоповідомлення, що забезпечується використаним математичним базисом.

Вбудова ДІ робиться шляхом використання нечутливих до збурних дій формальних параметрів матриці ЦЗ-контейнера – СНЧ її блоків малого розміру, отриманих шляхом її стандартної розбивки. Збільшення стійкості методу до збурних дій та забезпечення надійності сприйняття формованного стеганоповідомлення досягається шляхом збільшення максимального СНЧ блоку, задіяного в стеганоперетворенні, при цьому збурення СНЧ визначається за допомогою піднесення СНЧ блоків у натуральний ступінь *k*.

Алгоритмічна реалізація методу вимагає додаткових досліджень для встановлення значень параметрів *k* і Δ, над чим зараз працюють автори.

6. СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] M.E. Saleh, A.A. Aly, F.A. Omara, "Data security using cryptography and steganography techniques," *International Journal of Advanced Computer Science and Applications*, Vol. 7, Issue 6, pp. 390-397, 2016.

[2] S. Malalla, F.R. Shareef, "Novel approach for Arabic text steganography based on the "BloodGroup" text hiding method," *Engineering, Technology & Applied Science Research*, Vol. 7, Issue 2, pp. 1482-1485, 2017.

[3] В.Г. Грибунин, И.Н. Оков, И.В. Туринцев, *Цифровая стеганография*, М.: СОЛОН-Пресс, 2009. 272 с.

[4] D. Subhashini, P. Nalini, G. Chandrasekhar, "Comparison analysis of spatial Domain and compressed Domain steganographic techniques," *International Journal of Engineering Research and Technology*, Vol. 1, Issue 4, pp. 1-6, 2012.
[5] B. Li, "A survey on image steganography and steganalysis," *Journal of Information Hiding and Multimedia Signal Processing*, Vol. 2, Issue 2, pp. 142-172, 2011.
[6] S. Singh, T.J. Siddiqui, "A security enhanced robust steganography algorithm for data hiding," *International Journal of Computer Science Issues*, Vol. 9, Issue 3, pp. 131-139, 2012.
[7] S. Singh, T.J. Siddiqui, "Robust image steganography using complex wavelet transform," in *Proceedings of 2013 International Conference on Multimedia, Signal Processing and Communication Technologies*, Aligarh, India, 23-25 Nov. 2013, pp.56 – 60.
[8] М.А. Мельник, «Sign-нечувствительность сингулярных векторов матрицы изображения как основа стеганоалгоритма, устойчивого к сжатию», *Інформатика та математичні методи в моделюванні*, Том 3, № 2, С. 116-126, 2013.
[9] Z. Bao, X. Luo, Y. Zhang, C. Yang, F. Liu, "A robust image steganography on resisting JPEG compression with no side information," *IETE Technical Review*, Vol. 35, Issue 1, pp. 4-13, 2018.
[10] J. Tao, S. Li, X. Zhang, Z. Wang, "Towards robust image steganography," *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 29, Issue 2, pp. 594-600, 2019.
[11] Г.Ф. Конахович, А.Ю. Пузыренко, *Компьютерная стеганография: теория и практика*, К.: МК-Пресс, 2006. 288 с.
[12] А.А. Кобозева, М.А. Мельник, «Нечувствительность стеганосообщения к сжатию и формальные достаточные условия ее обеспечения», *Збірник наукових праць Військового інституту КНУ імені Тараса Шевченка*, № 38, С. 193-203, 2012.
[13] А.А. Кобозева, В.А. Хорошко, *Анализ информационной безопасности*, К.: ГУИКТ, 2009. 251 с.
[14] М.А. Мельник, «Стеганоалгоритм, устойчивый к сжатию», *Інформаційна безпека*, № 2(8), с. 99-106, 2012.
[15] Д. Деммель, *Вычислительная линейная алгебра: теория и приложения*, М.: Мир, 2001. 430 с.
[16] Р. Гонсалес, Р. Вудс, *Цифровая обработка изображений*, М.: Техносфера, 2006. 1070 с.
[17] C. Bergman, J. Davidson, "Unitary embedding for data hiding with the SVD," in *Proceedings of Security, Steganography, and Watermarking of Multimedia Contents VII*, Vol. 5681, pp. 619-630, 2005.
[18] A.A. Kobozeva, I.I. Bobok, A.I. Garbuz, "General principles of integrity checking of digital images and application for steganalysis," *Transport and Telecommunication*, Vol. 17, Issue 2, pp. 128-137, 2016.
[19] И.И. Бобок, «Теоретическое развитие общего подхода к проблеме выявления нарушений целостности цифровых контентов, основанного на анализе полного набора формальных параметров», *Інформатика та математичні методи в моделюванні*, Том 7, № 3, с. 170-177, 2017.
[20] І.І. Бобок, «Теоретичні основи методу виявлення порушення цілісності цифрового зображення в результаті накладання шуму», *Збірник наукових праць Військового інституту КНУ імені Тараса Шевченка*, № 63, С. 73-84, 2019.
[21] M.O. Kozina, "Steganographic method for solving a triple task", Матеріали *VII міжнародна науково-практична конференція «Проблеми та перспективи розвитку IT-індустрії»*, Харків, Україна, 17-18 квітня 2015 р., с. 32.
[22] T.H. The, T.L. Tien, "An efficient blind watermarking method based on significant difference of wavelet tree quantization using adaptive threshold," *International Journal of Electronics and Electrical Engineering*, Vol. 1, Issue 2, pp. 98-103, 2013.
[23] R.S. Run, S.J. Horng, W.H. Lin, T.W. Kao, and P. Fan, "An efficient wavelet-tree-based watermarking method," Expert Systems with Applications., Vol. 38, pp. 14357-14366, 2011.
[24] J.C. Patra, A.K. Kishore, C. Bornand, "Improved CRT-based DCT domain watermarking technique with robustness against JPEG compression for digital media authentication," in *Proceedings of 2011 IEEE International Conference on Systems, Man, and Cybernetics*, Anchorage, AK, USA, 9-12 Oct. 2011, pp. 2940–2945.
[25] Y.R. Wang, W.H. Lin, L. Yang, "An intelligent watermarking method based on particle swarm optimization," *Expert Systems with Applications*, Vol. 38, pp. 8024-8029, 2011.

***Кобозєва Алла Анатоліївна**, доктор технічних наук, професор, завідувач кафедри Інформатики і управління захистом інформаційних систем Одеського національного політехнічного університету.*

***Бобок Іван Ігорович**, кандидат технічних наук, доцент кафедри Інформаційних технологій проектування в електроніці й телекомунікаціях Одеського національного політехнічного університету.*