

**ВИКОРИСТАННЯ ТЕОРІЇ ГРАФІВ В УМОВАХ СЕЛЕКТИВНОЇ  
СТЕГANOГРАФІЇ**С. М. Григоренко<sup>1</sup>, А. А. Кобозєва<sup>2</sup>

---

<sup>1</sup>Національний університет «Одеська політехніка»  
1, Шевченка пр., Одеса, 65044, Україна  
<sup>2</sup>Одеський національний морський університет  
34, Мечникова вул., Одеса, 65029, Україна  
Email: alla\_kobozeva@ukr.net

---

Стеганографія є сьогодні одним з найпотужніших засобів захисту інформації, проте велика кількість сучасних стеганометодів мають обмеження області застосування, не розраховані на ефективну роботу з випадковим контейнером, який на сьогодні є найпоширенішим при практичному використанні стеганосистеми. Для рішення цієї проблеми використовується селективна стеганографія, яка значно покращує характеристики стеганосистеми, зокрема дозволяє зменшити спотворення контейнеру, в якості якого в роботі розглядається цифрове зображення, в результаті стеганоперетворення. На сьогодні проблеми селективної стеганографії не є достатньо дослідженими, відсутні загальні принципи селекції, які б не були розраховані на конкретні стеганоалгоритми, практично не розглядаються питання стійкості результату селекції до збурних дій. Метою даної роботи є удосконалення селективного методу, запропонованого авторами раніше, для підвищення стійкості результату селекції блоків до атак проти вбудованого повідомлення. Мета досягається шляхом побудови бінарного відношення нестроного порядку, визначеного на множині  $X$  непересічних блоків матриці контейнера, отриманих шляхом її стандартної розбивки, граф якого використовується для організації селекції блоків, при цьому кількісним критерієм для вибору блоку  $V$  є нормована відокремленість максимального сингулярного числа блоку  $VV^T$ . Найбільш важливим результатом роботи є розробка та застосування в запропонованому методі загальних принципів селекції блоків, що не є орієнтованими на конкретні стеганоалгоритми. Практична значимість отриманих результатів полягає в підвищенні стійкості результату селекції в умовах збурних дій, що забезпечується запропонованим методом, наслідком чого є підвищення ефективності стеганографічної системи в цілому.

**Ключові слова:** селективна стеганографія, бінарне відношення порядку, граф бінарного відношення, стійкість до збурних дій.

**Вступ.** Проблеми інформаційної безпеки та захисту інформації сьогодні є вкрай актуальними для України в умовах повномасштабної війни, яку розв'язала російська федерація, що включає, як складову, інформаційну агресію проти українського суспільства. Безпрецедентне зростання кібератак, інформаційно-психологічних операцій та цифрового шпигунства вимагає від держави, військових, критичної інфраструктури застосування найсучасніших та найнадійніших методів приховування та передачі даних.

Одним з найпотужніших засобів захисту інформації в умовах постійного зовнішнього моніторингу та аналізу трафіку є сьогодні стеганографія [1,2] – наука і мистецтво приховування інформації. На відміну від криптографії, результат застосування якої зразу «кидається в очі», представляючи «нечитабельний» контент, стеганографія приховує від третіх осіб сам факт передачі секретного повідомлення, що критично важливо для уникнення виявлення та протидії з боку супротивника. Проте велика кількість сучасних стеганометодів мають обмеження області застосування, вони не розраховані на ефективну роботу з випадковим контейнером, в якості якого далі розглядається цифрове зображення (ЦЗ), оскільки передбачають використання для

вбудови додаткової інформації (ДІ) всього контейнера чи його частин, зокрема блоків, обраних випадковим чином. Для деяких стеганометодів це несистематично призводить до невиконання певних вимог, що висуваються до відповідної стеганосистеми, при їх використанні, зокрема до порушення надійності сприйняття стеганоповідомлення, тобто до візуально помітної відмінності ЦЗ-контейнера від зображення, що несе в собі ДІ. Але саме випадковий контейнер є найпоширенішим для сучасних стеганосистем. Для покращення результату його використання довільним стеганометодом все більшого значення набуває селективна стеганографія, метою якої є обрання таких ділянок контейнера, які є найбільш сприятливими в тому чи іншому сенсі для стеганоперетворення, зокрема таких, що забезпечують відносно більший ступінь «непомітності» змін ЦЗ при вбудові ДІ в порівнянні з випадковим/довільним вибором ділянок контейнера для стеганоперетворення. Завдяки вибірковому підходу, селективна стеганографія дозволяє мінімізувати перцептивні спотворення на стеганоповідомленні, що є важливим для уникнення підозр з боку порушників.

Таким чином, дослідження, розробка та удосконалення методів селективної стеганографії є сьогодні критично актуальним завданням для забезпечення надійного та непомітного каналу передачі даних в умовах зовнішньої агресії та постійного кібернагляду.

**Стан проблеми.** На сьогоднішній день проблеми селективної стеганографії не є достатньо дослідженими: відсутні загальні принципи селекції, які б не були орієнтовані на конкретні стеганоалгоритми; часто селекція відбувається в просторовій області ЦЗ-контейнера, де визначальними критеріями відбору стають певні піксельні характеристики, а результатом – набір пікселів, хоча областю вбудови ДІ може слугувати область перетворення контейнера (частотна, області сингулярного, спектрального розкладання тощо); практично не розглядаються питання стійкості результату селекції до збурних дій.

Серед вимог до сучасної стеганографічної системи одною з основних є вимога забезпечення надійності сприйняття формованого стеганоповідомлення, в світлі чого і розглядатимуться можливості і переваги селективної стеганографії.

На сьогоднішній день найчастіше селекція областей ЦЗ-контейнера для вбудови ДІ зводиться до пошуку в ньому контурів [3-6]. Це є абсолютно природним, оскільки особливістю зорової системи людини є набагато більша ймовірність помітити зміни на зображенні в областях з малими перепадами значень яскравості, ніж в областях, де наявні контури, маленькі деталі, тобто перепади значень яскравості є значними. Підходи, що застосовуються в відповідних роботах, є різними: комплексне вейвлет-перетворення з подвійним деревом [3], де для стеганоперетворення використовуються коефіцієнти дискретного вейвлет-перетворення, а високочастотні області зображення ідентифікуються за допомогою методу виявлення контурів Кенні; детектор контурів Кірша [5]; в [4] використовується глибоке навчання, за допомогою якого отримується мапа контурів у вигляді двійкового зображення; в [6] контури виявляються за допомогою фільтра Собеля.

Хоча, з одного боку, виявлення контурів ЦЗ як результату селекції, як зазначено вище, є природним з урахуванням зазначеної мети відбору, з іншого боку, бажаним результатом тут є забезпечення покращення якісного/кількісного стану стеганоповідомлення для будь-якого зображення-контейнера, навіть, якщо це зображення взагалі не містить об'єктів/контурів, як, наприклад, отримане непрофесійною відеокамерою, представлено на рис.1. Для таких зображень орієнтація на контури, як області для вбудови ДІ, призведе до катастрофічного падіння (аж до 0 біт/піксель) пропускнуєї спроможності прихованого каналу зв'язку, що не дасть можливості використовувати їх в якості контейнерів, а тому такий селективний підхід принципово не може забезпечити можливість використання випадкового контейнера довільним стеганометодом. Крім того, цей підхід є досить «категоричним», однозначно

локалізуючи області вбудови ДІ в межах контурів, тим самим чітко обмежуючи зверху обсяг ДІ, яка може бути вбудована в контейнер.



**Рис. 1.** Оригінальне ЦЗ, що не містить контурів

Велика кількість сучасних селективних методів, зокрема і ті, що розглянуті вище, розроблені під метод модифікації найменшого значущого біта (LSB-метод) [7], що, на погляд авторів даної роботи, знижує цінність результатів, що представляються, оскільки, по-перше, це звужує область застосування селективного методу (чи вимагає додаткових досліджень для обґрунтування можливості/неможливості його використання під інші стеганометоди), по-друге, передбачає проведення стеганоперетворення лише в просторовій області контейнера, виключаючи стеганометоди, що працюють з областями перетворення, по-третє, LSB-метод сам по собі є таким, що забезпечує надійність сприйняття формованого стеганоповідомлення без будь-якої селекції.

Зауважимо, що, крім вже визначених недоліків, розглянуті вище роботи є показовими з точки зору існуючої загальної тенденції «ігнорування» складної проблеми, що залишається недостатньо дослідженою, хоча є критично важливою для організації ефективного декодування ДІ в умовах атак проти вбудованого повідомлення, тобто процесу, що є ключовим при організації прихованого каналу зв'язку, в умовах, що мають високу ймовірність: забезпечення стійкості результату проведеної селекції до збурних дій. Це питання майже не розглядається в межах селективної стеганографії.

Попіксельна селекція, представлена в роботах, згаданих вище, не завжди є виправданою не тільки по причині орієнтованості лише на просторове стеганоперетворення. На сьогодні найпоширенішими стеганографічними методами є блокові, де перед вбудовою ДІ матриця контейнера піддається розбивці на блоки, а селекція природно зводиться до вибору найбільш сприятливих для стеганоперетворення блоків. Один з найбільш ефективних блокових селективних методів, запропонований в [8], забезпечує, як заявляють автори, для відповідного стеганоповідомлення значення показника пікового відношення «сигнал-шум»  $PSNR$  61-65 dB навіть в умовах 80% модифікованих блоків. Запропонована схема розглядає виключно просторову область контейнера для стеганоперетворення, обираючи певний «регіон», при цьому цей вибір робиться серед пікселів в межах блоку. Метод вбудовує три біти ДІ в крайових пікселях з використанням мінімальної середньоквадратичної похибки для визначення можливості/неможливості залучення пікселів всередині блоку. Таким чином, авторами пропонується селективний метод під конкретний спосіб безпосередньої вбудови ДІ, не даючи уявлення про якість селекції у випадку застосування іншого методу стеганоперетворення.

Загальний селективний блоковий метод, тобто такий, який ніяк не орієнтований на використовуваний для стеганоперетворення стеганоалгоритм, був нещодавно представлений в [9]. Вибір відбувається серед блоків, отриманих шляхом стандартної розбивки [10] матриці ЦЗ, з метою збільшення ступеня надійності сприйняття стеганоповідомлення, що кількісно оцінюється за допомогою різницевого показника візуального спотворення  $PSNR$  [11], в порівнянні з випадковим використанням блоків. Основною кількісною характеристикою блоку  $B$  – критерієм, що використовувався для

вибору, була обґрунтовано обрана нормована відокремленість його максимального сингулярного числа. Даний метод дозволив значно збільшити показник  $PSNR$  для отримуваних стеганоповідомлень незалежно від використовуваного стеганометоду. Хоча в [9] питання забезпечення стійкості результату проведеної селекції до атак проти вбудованого повідомлення – збурних дій не розглядалося, враховуючи загальність і ефективність метода [9], доцільним є, зберігаючи його теоретичні основи, віднайти шляхи для вирішення означеного питання.

Метою роботи є удосконалення селективного методу, запропонованого в [9], що забезпечить підвищення стійкості результату селекції блоків до атак проти вбудованого повідомлення.

Для досягнення мети в роботі вирішуються наступні задачі:

1. Зміна принципу побудови бінарного відношення на множині блоків ЦЗ-контейнера відносно застосовуваного в [9] для уникнення негативних наслідків особливостей машинної арифметики та забезпечення повного впорядкування множини блоків;
2. Зміна критерію вибору блоків для підвищення стійкості селекції до атак проти вбудованого повідомлення;
3. Розробка удосконаленого селективного методу;
4. Оцінка ефективності запропонованого селективного методу.

**Вступні зауваження.** Для кращого розуміння шляхів удосконалення селективного методу [9] розглянемо детально спосіб організації вибору блоків, що ним реалізується.

Нормована відокремленість максимального сингулярного числа будь-якого блоку  $B$   $svdgap_n(1, B)$ , що є критерієм, який використовувався для вибору блоків в [9], визначається у відповідності з формулою:

$$svdgap_n(1, B) = \bar{\sigma}_1 - \bar{\sigma}_2, \quad (1)$$

де  $\bar{\sigma}_i = \frac{\sigma_i}{\|\sigma\|}$  – нормовані сингулярні числа (СНЧ),  $\sigma = (\sigma_1(B), \sigma_2(B), \dots, \sigma_l(B))$  – вектор

СНЧ  $B$ ,  $\|\cdot\|$  – Евклідова векторна норма,

Нормований вектор СНЧ

$$\bar{\sigma} = (\bar{\sigma}_1(B), \bar{\sigma}_2(B), \dots, \bar{\sigma}_l(B)) \quad (2)$$

Для організації селекції на множині  $X$  блоків ЦЗ-контейнера будувалося бінарне відношення  $\rho$  наступним чином: впорядкована пара  $\langle B_{ij}, B_{km} \rangle \in \rho$ , де  $B_{ij}, B_{km} \in X$ , якщо показники вкладу високочастотної складової, в якості яких застосовуються значення нормованої відокремленості максимальних СНЧ  $B_{ij}, B_{km}$ , будуть рівні:

$$B_{ij} \rho B_{km} \Leftrightarrow svdgap_n(1, B_{ij}) = svdgap_n(1, B_{km}). \quad (3)$$

Отримане бінарне відношення є відношенням еквівалентності, тому розбиває множину  $X$  на непересічні класи еквівалентності, в кожному з яких опиняються блоки контейнера, пов'язані відношенням  $\rho$ , а для будь-якої пари блоків з різних класів зв'язок їх в сенсі  $\rho$  є відсутнім. Відношенню  $\rho$  ставився у відповідність орієнтований граф, кожна компонента зв'язності якого визначала певний клас. За допомогою простої гомоморфної згортки вершин графа, що знаходилися в одній компоненті зв'язності, будувалася зважений макрограф, що відповідав ЦЗ-контейнеру, з макровершинами, що визначали класи еквівалентності блоків зображення. Вага макровершини відповідала значенню нормованої відокремленості максимального СНЧ блоків цього класу. Для вибору безпосередніх блоків для вбудови ДІ, що розглядалася як бінарна послідовність  $p_1, p_2, \dots, p_t$ ,  $p_i \in \{0, 1\}$ , визначалась загальна кількість  $T$  блоків контейнера, необхідних для вбудови наявної ДІ використовуваним стеганоалгоритмом. Для стеганоперетворення використовувалися  $T$  блоків, що відповідали макровершинам

побудованого макрографа контейнера, починаючи з макровершини з найменшою вагою (вклад високо-, середньочастотної складової в цих блоках є найбільшим, а тому ймовірність виникнення артефактів після вбудови ДІ є порівняно малою) в порядку зростання ваги вершин. Блоки з одного класу еквівалентності обиралися випадковим чином.

Принцип побудови бінарного відношення (3) не позбавлений недоліку: встановлення рівності для дійсних чисел  $svdgap_n(1, B_{ij})$ ,  $svdgap_n(1, B_{km})$ , що є результатами обчислень в системі чисел з плаваючою точкою, є нетривіальною задачею в силу скінченності множини таких чисел і, як наслідок, наявності обчислювальної похибки. І хоча всі СНЧ є добре обумовленими [12], що призводить до доброї обумовленості і нормованих відокремленостей максимальних СНЧ блоків, два природно рівних (нерівних) дійсних числа  $svdgap_n(1, B_{ij})$ ,  $svdgap_n(1, B_{km})$  в результаті обчислень можуть виявитися нерівними (рівними) в силу особливостей машинної арифметики. Для  $svdgap_n(1, B_{ij})$ ,  $svdgap_n(1, B_{km})$  по ходу організації процесу селекції у відповідності з [9] проводилось округлення до певної кількості значущих цифр, що є додатковим джерелом похибки в значеннях нормованої відокремленості максимального СНЧ блоку. Все вищезазначене об'єктивно може призвести до того, що блок контейнера опиниться не в тому класі еквівалентності, де він повинен бути природно, наслідком чого стануть похибки при побудові графа і відповідно макрографа ЦЗ-контейнера, знижуючи ефективність селекції.

**Принцип побудови бінарного відношення на множині блоків ЦЗ-контейнера.** Пропонується зміна принципа (3) побудови бінарного відношення  $\rho$  на множині  $X$  блоків ЦЗ-контейнера на наступний:

$$B_{ij} \rho B_{km} \Leftrightarrow svdgap_n(1, B_{ij}) \geq svdgap_n(1, B_{km}). \quad (4)$$

Можливість рівності для  $svdgap_n(1, B_{ij})$ ,  $svdgap_n(1, B_{km})$  для забезпечення  $B_{ij} \rho B_{km}$  в (4) залишається, що дозволяє сподіватися на збереженні всіх позитивних якостей селекції [9], але вона перестає бути єдиною визначальною властивістю.

Визначальна властивість (4) є менш чутливою до обчислювальної похибки, ніж (3), тому запропонована заміна сприятиме підвищенню стійкості результату селекції блоків в цілому до збурних дій, що підтверджується нижче результатами обчислювального експерименту.

Оскільки бінарне відношення (4) є рефлексивним, антисиметричним і транзитивним, воно є відношенням нестроого порядку. При цьому будь-які два блоки з множини  $X$  є порівняними по відношенню порядку  $\rho$ , що призведе до того, що відношення  $\rho$  визначає повний порядок на множині  $X$ .

Бінарному відношенню (4) поставимо у відповідність орієнтований зважений граф  $G(X, E)$ , де  $X$  – множина вершин,  $E$  – множина ребер, вершини якого відповідають блокам ЦЗ, а вага вершини дорівнює нормованій відокремленості його максимального СНЧ (1). Для наочності на рис.2 наведено приклад побудови  $G(X, E)$  для незначної за розміром частини ЦЗ (на рис.2(a) виділена червоним квадратом). Ваги вершин вказані всередині вершин.

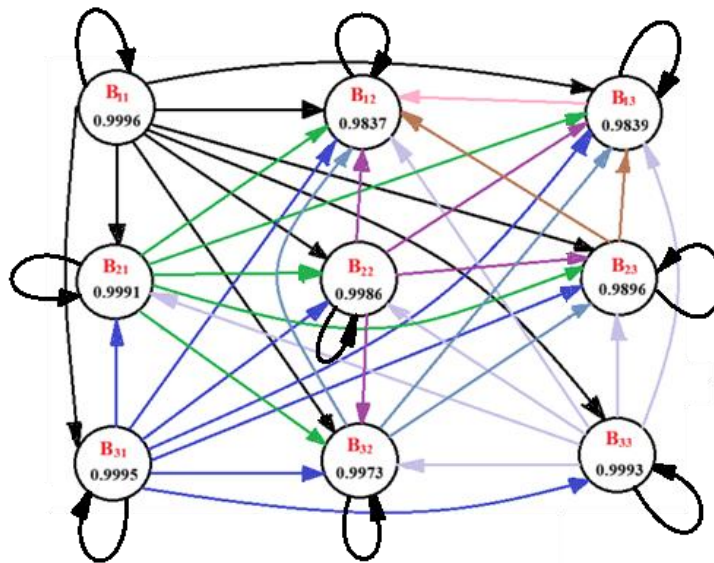
Оскільки граф  $G(X, E)$  є орієнтованим, для кожної вершини, можна визначити два локальних ступеня:  $\rho^+(B_{ij})$  - кількість ребер графа, інцидентних вершині  $B_{ij}$ , для яких вершина  $B_{ij}$  є початком,  $\rho^-(B_{ij})$  - кількість інцидентних вершині  $B_{ij}$  ребер, для яких  $B_{ij}$  є кінцем. Після того, як граф  $G(X, E)$  побудований, для селекції блоків сам кількісний критерій (1) вже непотрібний, оскільки вибір блоків пропонується реалізовувати з урахування лише  $\rho^+(B_{ij})$  і  $\rho^-(B_{ij})$  для кожної вершини.



а

60	60	58	58	62	65	70	70	68	71	59	48	68	95	131	161	146	123	140	155	156	153	152	152		
59	59	59	59	60	63	62	66	66	66	68	64	60	64	81	128	160	147	129	149	171	162	155	156		
59	60	60	61	61	63	63	64	64	61	64	65	65	61	56	66	113	148	143	149	160	164	159	160		
59	59	60	60	59	60	61	61	61	61	62	62	65	67	61	52	55	91	116	136	156	160	156	163		
58	58	57	57	B <sub>11</sub>	57	58	59	60	60	60	62	61	64	67	65	51	48	74	105	B <sub>13</sub>	129	157	164	159	
58	56	53	52	54	56	57	59	57	59	59	60	62	63	62	64	70	63	54	62	83	128	164	169		
57	54	54	53	53	54	56	57	56	59	60	59	59	59	60	57	67	86	76	65	59	73	121	159		
56	55	56	54	53	54	54	55	54	60	60	56	53	57	58	58	61	71	79	76	78	56	63	106		
56	57	55	54	52	53	55	53	54	57	57	52	54	56	57	58	59	60	68	72	75	78	62	56		
55	55	55	54	53	55	57	55	53	57	58	58	57	57	57	57	57	59	64	66	65	73	81	80		
55	53	56	57	56	53	56	60	57	57	59	59	58	57	57	57	55	54	59	62	62	66	74	83		
56	57	58	58	57	55	57	62	68	61	58	59	59	59	58	57	52	55	59	60	62	61	62	65		
57	58	59	59	B <sub>21</sub>	59	56	59	59	59	59	61	B <sub>22</sub>	68	70	60	58	58	57	58	59	B <sub>23</sub>	59	58	61	62
53	55	57	58	61	60	61	61	58	59	55	59	67	60	54	58	65	60	57	56	56	57	58	60		
51	53	54	57	62	62	63	64	60	55	53	56	58	59	55	60	83	93	67	55	57	57	57	57		
48	51	53	55	59	61	62	64	63	58	55	57	58	59	59	74	101	96	73	62	57	57	57	56		
49	50	53	54	57	58	62	63	63	58	55	56	57	58	63	69	74	72	68	62	59	58	56	55		
51	53	54	54	55	58	60	65	65	61	54	55	56	57	62	65	62	65	63	60	60	58	57	56		
54	55	56	57	59	59	61	62	69	71	62	56	54	58	61	62	60	57	58	57	56	55	56	56		
55	56	57	58	B <sub>31</sub>	59	60	59	62	67	71	73	62	55	59	59	57	54	53	55	56	56	55	55		
52	55	56	59	61	61	60	60	60	61	64	65	B <sub>33</sub>	63	61	59	54	55	55	55	B <sub>35</sub>	54	54	55		
53	55	58	62	62	62	61	59	55	58	60	61	62	63	60	56	57	56	56	55	55	55	54	53		
55	54	58	65	64	61	61	60	56	53	57	58	62	69	64	60	60	58	55	55	56	55	53	52		
57	55	58	60	60	60	60	58	56	56	57	55	58	70	65	61	61	59	58	58	57	55	52	51		

б



в

**Рис. 2.** Приклад побудови графа  $G(X, E)$  для ЦЗ: а – оригінальне ЦЗ, частина якого розміром  $24 \times 24$  пікселя використовується для побудови графа; б – матриця обраної частини ЦЗ з відповідною стандартною розбивкою на блоки; в – граф  $G(X, E)$

$G(X, E)$ .

При цьому схема збереження побудованого графа ЦЗ для організації такої селекції може бути організована в спрощеному вигляді, зберігаючи лише інформацію про ступені вершин. Крім того, саме повна впорядкованість множини  $X$ , що досягається завдяки введеному бінарному відношенню порядку, дозволяє провести додаткові спрощення для схеми збереження графа

Будь-які блоки ЦЗ є порівнянними по введеному бінарному відношенню  $\rho$ , з чого випливає, що загальна кількість ребер, інцидентних кожній вершині, буде дорівнювати  $N-1$ , без урахування петель, де  $N$  – загальна кількість блоків матриці ЦЗ. Наявні петлі, що відповідають кожній вершині графа, говорячи про рефлексивність бінарного

відношення, для проведення селекції блоків не відіграють ніякої ролі, оскільки відтворюють лише зв'язок блоку з самим собою, тому ці ребра далі не має сенсу враховувати, оскільки вони тільки ускладнюють загальну схему графа. Таким чином:

$$\rho^+(B_{ij}) + \rho^-(B_{ij}) = N - 1. \quad (5)$$

Враховуючи (5) при збереженні необхідної для селекції інформації про отриманий граф  $G(X, E)$  ЦЗ можна зберігати лише інформацію або про  $\rho^+(B_{ij})$ , або про  $\rho^-(B_{ij})$ . Таким чином, побудований на рис.2 граф може зберігатися у вигляді:

$$\begin{pmatrix} 8 & 0 & 1 \\ 5 & 4 & 2 \\ 7 & 3 & 6 \end{pmatrix} \quad \text{або} \quad \begin{pmatrix} 0 & 8 & 7 \\ 3 & 4 & 6 \\ 1 & 5 & 2 \end{pmatrix},$$

для  $\rho^+(B_{ij})$ ,  $\rho^-(B_{ij})$  відповідно. Найбільший пріоритет для вбудови ДІ мають блоки, яким відповідають найменші значення  $\rho^+(B_{ij})$  в першій матриці, найбільші значення  $\rho^-(B_{ij})$  в другій.

**Критерій вибору блоків для підвищення стійкості селекції до атак проти вбудованого повідомлення.** Для селективної стеганографії важливим є стійкість відповідного алгоритму до збурних дій – атак: селективний алгоритм повинен бути таким, щоб навіть в умовах атаки зберегти можливість відновлення блокового стеганошляху під час декодування ДІ. Оскільки кількісним критерієм для вибору блоку є нормована відокремленість його максимального СНЧ (1), яка, як вже було зазначено вище, є добре обумовленою, то її зміни при збуреннях блоків будуть незначними. Але самі по собі значення нормованої відокремленості при обраному способі селекції не відіграють ключової ролі після побудови  $G(X, E)$ : для забезпечення можливості ефективного декодування ДІ після атак ключовим буде не абсолютна зміна значень (1), а відносне співвідношення між значеннями цього параметру у блоків. Таким чином, для забезпечення можливості ефективного відновлення ДІ граф ЦЗ  $G(X, E)$  повинен залишитися без змін, в порівнянні з його первісним видом, при цьому зміни нормованої відокремленості можуть відбуватися. Ця ідея є основною для побудови селективного блокового методу, що пропонується в роботі. Вона і надалі буде використовуватися авторами як загальна ідея ефективної селекції: після забезпечення стійкості нової «похідної» структури, що відповідає ЦЗ і несе інформації про його блокові зв'язки у відповідності з обраним критерієм (в даному випадку похідна структура – це  $G(X, E)$ ), для якої основними є її якісні характеристики, безпосередній кількісний критерій стає непотрібним, його можна відкинути. Але ключовим моментом тут є попереднє забезпечення стійкості похідної структури.

В [13,14] доведено, що нормований вектор СНЧ  $\bar{\sigma}$  (2), що відповідає довільному  $l \times l$  – блоку  $B$ , будучи нечутливим, має більшу чутливість до збурних дій, ніж також нечутливий нормований вектор

$$\bar{\sigma} = \left( \bar{\sigma}_1(BB^T), \bar{\sigma}_2(BB^T), \dots, \bar{\sigma}_l(BB^T) \right) = \frac{\sigma_{BB^T}}{\|\sigma_{BB^T}\|}, \quad (6)$$

де  $\sigma_{BB^T} = (\sigma_1(BB^T), \sigma_2(BB^T), \dots, \sigma_l(BB^T))$  - вектор СНЧ  $BB^T$ . Враховуючи це, для підвищення стійкості структури графа  $G(X, E)$  до збурних дій, що застосовуються до відповідного ЦЗ, пропонується в якості визначального для вибору блоків параметру використовувати не (1), а нормовану відокремленість максимального СНЧ перетвореного блоку  $BB^T$ , для якого показано [13,14]:  $\sigma_i(BB^T) = \sigma_i^2(B)$ ,  $i = \overline{1, l}$ .

**Розробка удосконаленого селективного методу.** З урахуванням всього вищенаведеного пропонується наступний селективний метод вибору блоків ЦЗ-контейнера для вбудови ДІ.

**Крок 1.** Матриця  $F$  ЦЗ-контейнера розміром  $m \times n$  розбивається стандартним чином на непересічні  $l \times l$ -блоки  $B_{ij}$ ,  $i = 1, \overline{\left\lfloor \frac{m}{l} \right\rfloor}$ ,  $j = 1, \overline{\left\lfloor \frac{n}{l} \right\rfloor}$ , де  $[\cdot]$  - ціла частина аргументу.

**Крок 2.** Для  $\forall B_{ij}$ ,  $i = 1, \overline{\left\lfloor \frac{m}{l} \right\rfloor}$ ,  $j = 1, \overline{\left\lfloor \frac{n}{l} \right\rfloor}$  робити:

2.1. Знайти сингулярний спектр блоку  $B_{ij}B_{ij}^T$ :

$$\sigma_1(B_{ij}B_{ij}^T) \geq \sigma_2(B_{ij}B_{ij}^T) \geq \dots \geq \sigma_l(B_{ij}B_{ij}^T) \geq 0;$$

2.2. Сформувати вектор (6):  $\overline{\sigma} = \left( \overline{\sigma}_1(B_{ij}B_{ij}^T), \overline{\sigma}_2(B_{ij}B_{ij}^T), \dots, \overline{\sigma}_l(B_{ij}B_{ij}^T) \right) = \frac{\sigma_{B_{ij}B_{ij}^T}}{\left\| \sigma_{B_{ij}B_{ij}^T} \right\|}$ ,

де  $\sigma_{B_{ij}B_{ij}^T} = \left( \sigma_1(B_{ij}B_{ij}^T), \sigma_2(B_{ij}B_{ij}^T), \dots, \sigma_l(B_{ij}B_{ij}^T) \right)$ ;

2.3. Знайти нормовану відокремленість  $svdgap_n(1, B_{ij}B_{ij}^T)$  максимального СНЧ блоку  $B_{ij}B_{ij}^T$ :

$$svdgap_n(1, B_{ij}B_{ij}^T) = \overline{\sigma}_1(B_{ij}B_{ij}^T) - \overline{\sigma}_2(B_{ij}B_{ij}^T). \quad (7)$$

**Крок 3.** На множині  $X$  блоків ЦЗ визначити бінарне відношення  $\rho$  нестрогого порядку у відповідності з (4), яке для  $B_{ij}B_{ij}^T$  буде виглядати:

$$B_{ij}\rho B_{km} \Leftrightarrow svdgap_n(1, B_{ij}B_{ij}^T) \geq svdgap_n(1, B_{km}B_{km}^T).$$

**Крок 4.** Для бінарного відношення  $\rho$  побудувати відповідний граф  $G(X, E)$ , де  $X$  - множина вершин,  $E$  - множина ребер, при цьому, враховуючи повну впорядкованість множини  $X$ , маємо:  $|X| = \left\lfloor \frac{n}{l} \right\rfloor \cdot \left\lfloor \frac{m}{l} \right\rfloor$ ,  $|E| = \frac{1}{2} \cdot \left( \left\lfloor \frac{n}{l} \right\rfloor \cdot \left\lfloor \frac{m}{l} \right\rfloor - 1 \right) \cdot \left\lfloor \frac{n}{l} \right\rfloor \cdot \left\lfloor \frac{m}{l} \right\rfloor + \left\lfloor \frac{n}{l} \right\rfloor \cdot \left\lfloor \frac{m}{l} \right\rfloor$  (з урахуванням петель), де  $|\cdot|$  - потужність множини.

**Крок 5.** Для кожної вершини  $B_{ij}$  графа  $G(X, E)$  визначити ступені  $\rho^+(B_{ij})$ ,  $\rho^-(B_{ij})$  без врахування петель.

**Крок 6.** Сформувати схему графа, інформативну для проведення селекції блоків:

$$\left( \begin{array}{cccc} \rho^+(B_{11}) & \rho^+(B_{12}) & \dots & \rho^+\left(B_{1, \left\lfloor \frac{m}{l} \right\rfloor}\right) \\ \rho^+(B_{21}) & \rho^+(B_{22}) & \dots & \rho^+\left(B_{2, \left\lfloor \frac{m}{l} \right\rfloor}\right) \\ \dots & \dots & \dots & \dots \\ \rho^+\left(B_{\left\lfloor \frac{n}{l} \right\rfloor, 1}\right) & \rho^+\left(B_{\left\lfloor \frac{n}{l} \right\rfloor, 2}\right) & \dots & \rho^+\left(B_{\left\lfloor \frac{n}{l} \right\rfloor, \left\lfloor \frac{m}{l} \right\rfloor}\right) \end{array} \right) \left( \begin{array}{c} \text{або} \\ \left( \begin{array}{cccc} \rho^-(B_{11}) & \rho^-(B_{12}) & \dots & \rho^-\left(B_{1, \left\lfloor \frac{m}{l} \right\rfloor}\right) \\ \rho^-(B_{21}) & \rho^-(B_{22}) & \dots & \rho^-\left(B_{2, \left\lfloor \frac{m}{l} \right\rfloor}\right) \\ \dots & \dots & \dots & \dots \\ \rho^-\left(B_{\left\lfloor \frac{n}{l} \right\rfloor, 1}\right) & \rho^-\left(B_{\left\lfloor \frac{n}{l} \right\rfloor, 2}\right) & \dots & \rho^-\left(B_{\left\lfloor \frac{n}{l} \right\rfloor, \left\lfloor \frac{m}{l} \right\rfloor}\right) \end{array} \right) \end{array} \right). \quad (8)$$

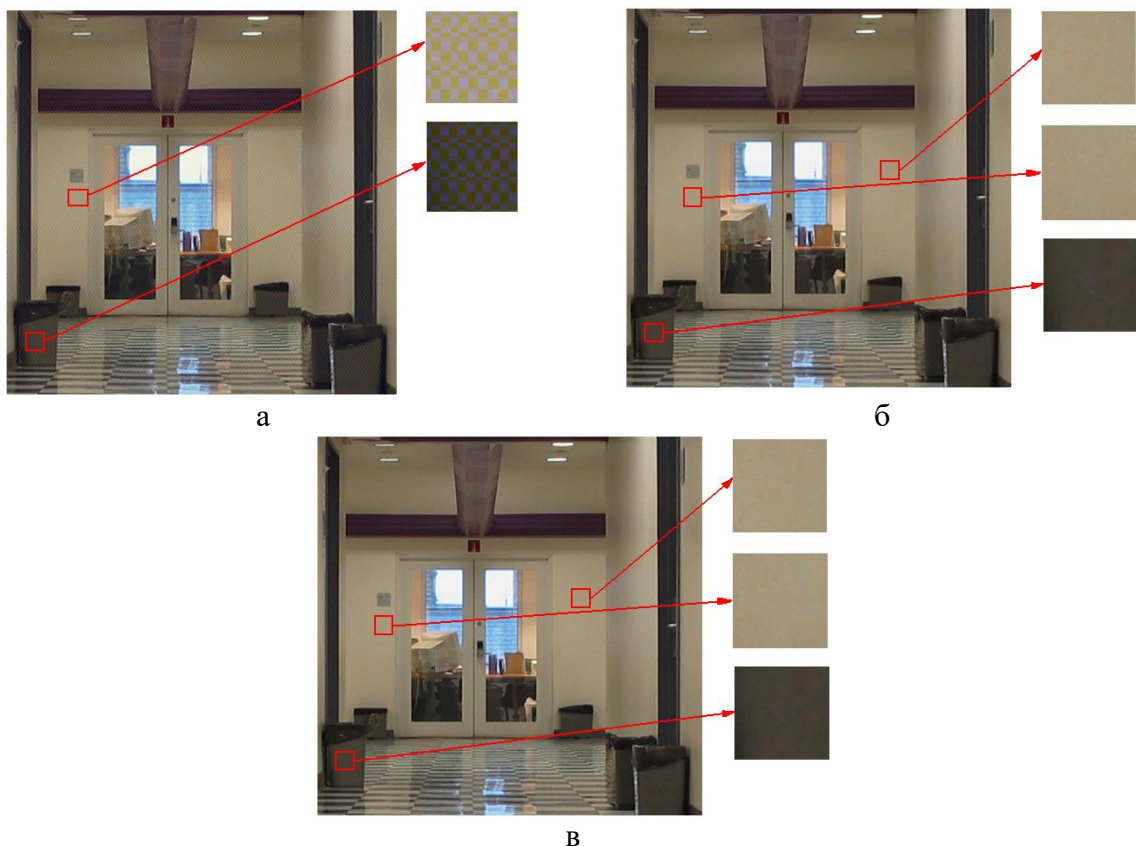
**Крок 7.** Розрахувати кількість  $T$  блоків ЦЗ-контейнера, необхідних для вбудови отриманої в результаті роботи прекодера стегаючої системи ДІ у відповідності з використовуваним стегаючим методом.

**Крок 8.** Для стеганоперетворення використати перші  $T$  блоків, для яких відповідні значення елементів  $\rho^+(B_{ij})$  ( $\rho^-(B_{ij})$ ) в матриці (8) є найменшими (найбільшими).

Для порівняльної оцінки ефективності запропонованого методу селекції і методу [9] був проведений обчислювальний експеримент, в ході якого формувалася випадковим чином бінарна послідовність, яка виступала в якості ДІ. Як стеганометоди для вбудови ДІ в експерименті були задіяні: один з найбільш стійких до атаки стиском стеганографічний метод [15], який призводить до несистематичного виникнення артефактів на ЦЗ-стеганоповідомленні; один з найбільш широко використовуваних і модифікованих методів - Коха і Жао [11], порушення надійності сприйняття в якому може мати місце зі збільшенням параметра, що використовується при модифікації коефіцієнтів дискретного косинусного перетворення при вбудові біта ДІ в черговий блок. Ці методи навмисно брались такими ж, як і в [9]. В експерименті було задіяно 200 ЦЗ з бази 4cam\_auth [16] (формат Tif), 200 ЦЗ з бази img\_Nikon\_D70s [17] (формат Tif), 100 ЦЗ, отриманих непрофесійними відеокамерами (формат Tif), 500 ЦЗ з бази NRCS [18] (формат Jpeg). Множину отриманих ЦЗ позначимо  $M$ .

При проведенні експерименту стеганоперетворення кожного контейнера проводилось трьома різними способами, що відрізнялися вибором блоків для вбудови ДІ: випадковий вибір блоків; селекція блоків у відповідності з [9]; селекція блоків у відповідності з запропонованим у роботі методом.

Типові результати експерименту продемонстровані на рис.3 (навмисно для демонстрації використовується ЦЗ, що було використано для демонстрації і в [9]). Очевидним є факт покращення візуального сприйняття ЦЗ-стеганоповідомлень, сформованих з застосуванням селективних методів, в порівнянні з випадковим вибором блоків.



**Рис. 3.** Результати стеганоперетворення за допомогою стеганометода Коха і Жао: а – стеганоповідомлення, при формуванні якого блоки обирались випадково; б – стеганоповідомлення, сформоване з попередньою селекцією блоків [9]; в – стеганоповідомлення, де селекція блоків робилася запропонованим в роботі методом

Запропонований спосіб селекції блоків дозволяє покращити стійкість результату селекції в умовах атак проти вбудованого повідомлення, зокрема в умовах атаки стиском. Мається на увазі наступне. Для селективної стеганографії велике значення має питання синхронізації: забезпечення механізмів, які дозволяють ідентифікувати початок і послідовність використаних для вбудови додаткової інформації пікселів/блоків контейнера при організації процесу декодування. Один з таких механізмів передбачає проводити вбудову ДІ таким чином, щоб визначальний параметр (критерій селекції) блоку залишався незмінним після стеганоперетворення. Необхідно зазначити, що загалом в блоках стеганоповідомлення в разі, якщо воно зазнало збурної дії, цей визначальний параметр може змінитися, наслідком чого можуть бути значні утруднення при визначенні тих блоків і їх послідовності, що використовувалися під час стеганоперетворення, для організації процесу декодування ДІ. В нашому випадку може зазнати збурень граф  $G(X, E)$  і матриця (8). Але коли в якості визначального параметру використовується (7) замість (1), то збільшення стійкості критерію селекції шляхом використання перетвореного блоку призведе очевидно і до збільшення стійкості результату селекції блоків. Для практичного підтвердження цього було проведено обчислювальний експеримент, в якому були задіяні ЦЗ з множини  $M$ . Всі ЦЗ на цьому етапі експерименту обрізалися до розміру  $400 \times 400$ , розбивка проводилася стандартним чином на  $8 \times 8$ -блоки. Враховуючи, що найбільш поширеною атакою проти вбудованого повідомлення сьогодні є атака стиском, основна увага при проведенні обчислювального експерименту приділялася саме цій атаці. Результати експерименту, які повністю підтверджують теоретичні міркування про перевагу (7) в порівнянні з (1), наведені в табл.1,2.

Таблиця 1

Результати порівняльного аналізу стійкості селекції блоків за допомогою запропонованого методу з різними визначальними параметрами в умовах атаки стиском

Визначальний параметр селекції блоків	Кількість ЦЗ (%), для яких спостерігалися зміни в матриці (8) в результаті атаки стиском з коефіцієнтом якості $QF$		
	$QF=80$	$QF=85$	$QF=90$
(1)	9.1	6.5	1.7
(7)	4.9	4.3	1.2

Таблиця 2

Результати порівняльного аналізу стійкості селекції блоків за допомогою запропонованого методу з різними визначальними параметрами в умовах накладання шуму

Визначальний параметр селекції блоків	Кількість ЦЗ (%), для яких спостерігалися зміни в матриці (8) в результаті накладання шуму	
	Гауссівського з $D = 0.00001$	Мультиплікативного з $D = 0.0001$
(1)	5.1	4.1
(7)	5.3	2.0

Результати порівняльного аналізу селективного методу [9] та його запропонованої модифікації дали порівняно однакові результати з точки зору надійності сприйняття стеганоповідомлення, що оцінювалася за допомогою суб'єктивного ранжування: стеганоповідомлення, що отримувалися з використанням обговорюваних селективних методів за допомогою однакових стеганографічних алгоритмів і однакової ДІ, візуально не розрізнялись. При цьому встановлено:

- кількісний показник (PSNR) візуального спотворення контейнера в результаті стеганоперетворення з попереднім застосуванням селекції блоків як первісним, так і удосконаленим запропонованим в роботі методом ніде не був менше цього показника для стеганоповідомлення, отриманого при випадковому виборі блоків для вбудови ДІ;

- при застосуванні кожного з обговорюваних селективних методів вдалося підвищити значення PSNR на 2-6 dB, але для первісного методу [9] таке значне підвищення мало місце для 54% ЦЗ, тоді як для удосконаленого – для 59% ЦЗ з множини  $M$ . Такий результат є наслідком зміни принципу побудови бінарного відношення з (3) на (4), який зменшив вплив обчислювальної похибки на структуру остаточного графа, що ставиться у відповідність ЦЗ;
- зміна кількісного критерію вибору блоків з (1) на (7) дала можливість підвищити стійкість результату селекції блоків в умовах збурних дій на стеганоповідомлення, забезпечуючи стійкість відповідного графу ЦЗ (табл.1,2).

**Висновки.** В роботі вирішено важливу науково-практичну задачу підвищення стійкості результату селекції блоків до збурних дій незалежно від використовуваного для вбудови ДІ стеганометоду, шляхом удосконалення селективного методу, запропонованого авторами раніше.

Запропонований спосіб селекції заснований на використанні графа  $G(X, E)$  бінарного відношення нестроого порядку, визначеного на множині  $X$  непересічних блоків матриці ЦЗ, отриманих шляхом її стандартної розбивки. Введене бінарне відношення визначає повний порядок на множині  $X$ , дозволяє зменшити вплив обчислювальної похибки на структуру остаточного графа, що ставиться у відповідність ЦЗ. Результатом цього є зростання, в порівнянні з прототипом, на 5% загальної кількості ЦЗ, де збільшення значення PSNR виявилось значним (аж до 6 dB).

Запропонований удосконалений селективний метод, як і прототип [9], є загальним, тобто таким, результат роботи якого не пов'язаний безпосередньо з використовуваним для вбудови ДІ стеганометодом.

В якості кількісного критерія для вибору блоків в удосконаленому методі використовується нормована відокремленість максимального СНЧ не первісного блоку  $B$  ЦЗ-контейнера, як в прототипі, а результату його перетворення – блоку  $B^T B$ , що дозволило підвищити максимально стійкість результату селекції в умовах збурних дій: на 4.2% в умовах атаки стиском, на 1.9% в умовах накладання шуму.

Отримані кількісні показники практичної роботи запропонованого селективного методу говорять про забезпечення підвищення ефективності стеганографічної системи в цілому при його використанні.

#### Список літератури

1. Srinivasan D. et al. A comprehensive review on advancements and applications of steganography. 2024. URL: <https://doi.org/10.13140/RG.2.2.13568.44807>.
2. Abdulla A.A. Digital image steganography: challenges, investigation, and recommendation for the future direction. *Soft Computing*. 2024. 28, P. 8963–8976.
3. Kadhim I.J., Premaratne P., Vial P.J. Adaptive Image Steganography Based on Edge Detection Over Dual-Tree Complex Wavelet Transform. *Proceedings of the 14<sup>th</sup> International Conference on Intelligent Computing Methodologies (ICIC 2018)*, Wuhan, China, 2018. Part III. P. 544–550.
4. Ray B. et al. Image steganography using deep learning based edge detection. *Multimedia Tools and Applications*. 2021. 80. P. 33475–33503.
5. Ghosal S.K., Chatterjee A., Sarkar R. Image steganography based on Kirsch edge detection. *Multimedia Systems*. 2021. 27. P. 73–87.
6. Sarrafpour B.A.S. et al. An Adaptive Edge-Based Steganography Algorithm for Hiding Text into Images. *Proceedings of the 2021 IEEE 19<sup>th</sup> International Conference on Embedded and Ubiquitous Computing (EUC)*, Shenyang, China, 2021. P. 109–116.
7. Aslam M.A. et al. Image Steganography using Least Significant Bit (LSB) — A Systematic Literature Review. *Second International Conference on Computing and Information Technology (ICCIT)*, Tabuk, Saudi Arabia. 2022. P. 32–38.

8. Laishram D., Tuithung T. A novel minimal distortion-based edge adaptive image steganography scheme using local complexity. *Multimedia Tools and Applications*. 2021. 80. P. 831–854.
9. Bobok I.I. et al. Application of graph theory to ensure the reliability of steganographic message perception in the creation of a covert communication channel. *Proceedings of the 13-th International Conference on Information Control Systems & Technologies. Odesa, Ukraine*. 2025. P.94-108.
10. Gonzalez R., Woods R. *Digital Image Processing* (4<sup>th</sup> Ed.). Pearson, 2018. 1020 p.
11. Конахович Г.Ф., Прогонов Д.О., Пузиренко О.Ю. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних. Київ: Alex Print Centre, 2018. 558 с.
12. Demmel J.W. *Applied Numerical Linear Algebra*. SIAM, 1996. 420 p.
13. Бобок І.І. Дослідження властивостей формальних параметрів цифрового зображення в умовах порушення його цілісності. *Сучасна спеціальна техніка*. 2017. № 4(51). С. 6–16.
14. Бобок І.І. Дослідження параметрів перетворених блоків цифрового зображення для виявлення порушення його цілісності. *Інформатика та математичні методи в моделюванні*. 2022. № 12(3). С. 161–170.
15. Melnik M. Compression-resistant steganography algorithm. *Information Security*. 2012. No.2. P. 99–106.
16. Hsu Y., Chang S. Detecting image splicing using geometry invariants and camera characteristics consistency. *IEEE International Conference on Multimedia and Expo*, Toronto. 2006. P. 549–552.
17. Gloe T., Böhme R. The Dresden Image Database for benchmarking digital image forensics. *ACM Symposium on Applied Computing*. New York. 2010. P. 1585–1591.
18. NRCS Photo Gallery. USDA.com. URL: <https://www.nrcs.usda.gov>

С. М. Григоренко, А. А. Кобозєва

## GRAPH THEORY APPLICATION FOR ENHANCED SELECTIVE STEGANOGRAPHY

S.M. Grigorenko<sup>1</sup>, A.A.Kobozieva<sup>2</sup>

<sup>1</sup>National Odesa Polytechnic University  
1, Shevchenko Ave., Odesa, 65044, Ukraine

<sup>2</sup>Odesa National Maritime University,  
34, Mechnykova Str., Odesa, 65029 Ukraine  
Email: alla\_kobozeva@ukr.net

Steganography is currently one of the most powerful means of information security. However, a large number of modern steganographic methods have limited applicability and are not designed for effective operation with a random container, which is the most common case in the practical use of a steganographic system today. To solve this problem, selective steganography is used, which significantly improves the characteristics of the steganographic system, particularly by allowing for the reduction of container distortion resulting from the steganographic transformation, where a digital image is considered as the container in this work. Currently, the problems of selective steganography are not sufficiently investigated; general selection principles that are not tailored to specific steganographic algorithms are lacking, and issues of the robustness of the selection result against disruptive actions are practically not considered. The goal of this work is the improvement of the selective method previously proposed by the authors to increase the robustness of the block selection result against attacks targeting the embedded message. This goal is achieved by constructing a binary non-strict order relation defined on the set  $X$  of non-overlapping blocks of the container matrix, obtained by its standard partitioning, the graph of which is used to organize the block selection. The quantitative criterion for selecting a block  $B$  is the normalized separability of the maximum singular value of the block  $BB^T$ . The most important result of the work is the development and application of general block selection principles in the proposed method, which are not oriented toward specific steganographic algorithms. The practical significance of the obtained results lies in increasing the robustness of the selection result under disruptive actions, which is ensured by the proposed method, consequently leading to an increase in the efficiency of the steganographic system.

**Keywords:** selective steganography, binary order relation, graph of a binary relation, robustness against disruptive actions.