



Алла КОБОЗЄВА, д-р техн. наук, проф.

ORCID ID: 0000-0001-7888-0499

e-mail: alla_kobozeva@ukr.net

Одеський національний морський університет, Одеса, Україна

Світлана ГРИГОРЕНКО, канд. техн. наук

ORCID ID: 0009-0006-4551-8243

e-mail: sngrygorenko@gmail.com

Національний університет "Одеська політехніка", Одеса, Україна

ПРОБЛЕМА СИНХРОНІЗАЦІЇ В СЕЛЕКТИВНІЙ СТЕГАНОГРАФІЇ

Вступ. Селективна стеганографія нині є потужним інструментом для покращення характеристик стеганографічної системи, зокрема в умовах використання випадкового контейнера. Однією з основних нерозв'язаних проблем сучасної селективної стеганографії залишається проблема синхронізації: забезпечення механізмів, які дають змогу ідентифікувати початок і послідовність використаних для вбудови додаткової інформації пікселів / блоків контейнера в організації процесу декодування. Метою роботи є підвищення ефективності стеганосистеми з допомогою забезпечення синхронізації в умовах застосування селекції блоків, загальні принципи якої запропоновані авторами раніше.

Методи. Використано: селективні методи вибору блокового стеганошляху, загальний підхід до аналізу стану інформаційних систем для дослідження впливу стеганоперетворення на блоки зображення-контейнера та вибору критерію селекції блоків, методи теорії збурень для оцінювання можливих меж змін сингулярних чисел блоків, методи сучасної стеганографії.

Результати. Обґрунтовано доцільність принципу синхронізації шляхом забезпечення незмінності визначального параметра (критерію селекції) блока після стеганоперетворення. Запропоновано метод, що реалізує обраний спосіб синхронізації в умовах селекції блоків, який не залежить від використовуваного стеганографічного методу, заснований на модифікації сингулярного спектра блока для забезпечення незмінності нормованої відокремленості максимального сингулярного числа – кількісного критерію селекції.

Висновки. Застосування запропонованого механізму синхронізації в умовах селекції блоків контейнера з метою забезпечення надійності сприйняття стеганоповідомлення дало змогу підвищити ефективність стеганосистеми на 4.1–4.3 dB під час використання випадкових контейнерів, причому запропонований спосіб синхронізації не потребує розширення секретного ключа та його додаткової передачі, збереження додаткової інформації про отриманий стеганошлях.

Ключові слова: селективна стеганографія, синхронізація, цифрове зображення, сингулярне число, випадковий контейнер.

Вступ

Стеганографія нині є одним з найефективніших засобів захисту інформації, який використовується в багатьох сферах людської діяльності, зокрема й у медицині, фінансовому, банківському секторі, у захисті інтелектуальної власності тощо. Стеганографію називають мистецтвом прихованої комунікації, підкреслюючи той факт, що вона забезпечує непомітність для третіх осіб наявності додаткової інформації в тому чи іншому інформаційному контенті – контейнері, який сам по собі не привертає уваги (Charan, 2023).

Дослідники в цій галузі досягли значних успіхів, але деякі проблеми залишаються такими, що потребують залучення нових математичних інструментів, розроблення нових підходів до їх розв'язання. Серед таких загальних проблем є розвиток і вдосконалення селективної стеганографії (Naji et al., 2020; Taher et al., 2022).

Селективна стеганографія сьогодні є актуальним напрямом для покращення якісних і кількісних характеристик стеганографічної системи, оскільки передбачає вибір за певними критеріями таких частин контейнера для вбудови додаткової інформації (ДІ), що забезпечують кращий у певному сенсі результат стеганоперетворення. Це може бути зменшення візуальних спотворень, зменшення чутливості стеганоповідомлення до атак тощо (Sarrafpour et al., 2021).

Всі стеганографічні контейнери можна розподілити на три типи: вибіркові, випадкові та нав'язані. Нині найбільш поширеними інформаційними контентами, що використовуються як контейнери в сучасній стеганографії, виступають цифрові зображення (ЦЗ), які далі розглянуто в роботі. Найкращі властивості отриманого стеганоповідомлення очевидно забезпечує вибірковий контейнер, але саме випадковий контейнер є найпоширенішим у організації прихованого каналу зв'язку, незалежно від наявних у нього властивостей, які можуть значно знижувати ефективність стеганоперетворення чи говорити про недоцільність його використання як контейнера, наприклад, ЦЗ, що має значні ділянки з незначними перепадами значень яскравості пікселів (Kadhim, Premaratne, & Vial, 2018). Селективна стеганографія частково розв'язує означену проблему: очевидно, що вибір найбільш придатних областей навіть випадкового контейнера для вбудови ДІ дозволить підвищити якісну картину стеганоповідомлення, порівняно з випадковим вибором областей для стеганоперетворення, що робить селективну стеганографію актуальним напрямом у галузі сучасного захисту інформації.

Нині проблеми селективної стеганографії потребують подальшого розвитку й удосконалення: відсутні загальні принципи селекції; часто селекція відбувається в просторовій області ЦЗ-контейнера, хоча для стеганоперетворення може використовуватися частотна, області сингулярного, спектрального розкладання матриці тощо; практично не піднімається питання синхронізації – забезпечення механізмів, які дозволяють ідентифікувати початок і послідовність використаних для вбудови додаткової інформації пікселів / блоків контейнера у організації процесу декодування, без яких останній є неможливим.



Метою статті є підвищення ефективності роботи стеганографічної системи шляхом забезпечення синхронізації в умовах застосування селекції блоків, загальні принципи якої запропоновано в дослідженнях (Kobozieva et al., 2025; Бобок, & Кобозева, 2025).

Під ефективністю стеганосистеми в роботі розуміють забезпечення надійності сприйняття стеганоповідомлення, кількісною оцінкою якої є поширений в області стеганографії показник візуального спотворення контейнера – пікове відношення "сигнал–шум" PSNR (Конахович, Прогонов, & Пузиренко, 2018).

Для досягнення мети в роботі розв'язують такі задачі: вибір принципу синхронізації в умовах селекції блоків (Kobozieva et al., 2025; Бобок, & Кобозева, 2025); розроблення відповідного методу, що реалізує обраний спосіб синхронізації.

Методи

В роботі використовують такі підходи та методи дослідження:

1. Аналіз відкритих джерел та огляд сучасного стану селективної стеганографії для визначення існуючих тут проблем.

2. Загальний підхід до аналізу інформаційних систем (ЗПАІС) заснований на теорії збурень і матричному аналізі, який слугує базою для дослідження впливу стеганоперетворення на блоки зображення-контейнера, зокрема на їхні сингулярні числа, та використовується для вибору критерію селекції блоків.

3. Методи теорії збурень для оцінювання можливих меж змін сингулярних чисел блоків зображення.

4. Селективні методи вибору блокового стеганошляху.

5. Методи сучасної стеганографії у проведенні обчислювальних експериментів.

Огляд літератури. До стеганосистеми нині висувають значну кількість вимог, причому однією з основних є вимога забезпечення надійності сприйняття стеганоповідомлення, яка полягає в тому, що візуально воно не повинно відрізнятися від порожнього контейнера. Шляхи задоволення саме цієї вимоги за допомогою селективної стеганографії розглянуто в цій статті.

На сьогодні найчастіше селекція областей ЦЗ-контейнера для вбудови ДІ зводиться до пошуку в ньому контурів. У роботі (Kadhim, Premaratne, & Vial, 2018) запропоновано метод, заснований на виявленні контурів у ЦЗ за допомогою комплексного вейвлет-перетворення з подвійним деревом. Для стеганоперетворення використовують коефіцієнти дискретного вейвлет-перетворення. Високочастотні області зображення ідентифікують за методом виявлення контурів Кенні. Переважна більшість бітів ДІ вбудовується в сильно текстуровані області, завдяки чому візуальні спотворення ЦЗ в результаті стеганоперетворення є незначними.

Вибір саме контурів у ЦЗ-контейнері як найбільш сприятливої області для вбудови ДІ для забезпечення надійності сприйняття стеганоповідомлення зроблено також у роботах (Ghosal, Chatterjee, & Sarkar, 2021; Ray, Mukhopadhyay, & Hossain, 2021; Sarrafpour et al., 2021), де для пошуку використано різні підходи і принципи. Наприклад, у дослідженні (Ghosal, Chatterjee, & Sarkar, 2021) застосовано детектор контурів Кірша, причому для безпосередньої вбудови ДІ тут використано метод модифікації найменшого значущого біта – LSB-метод (Aslam, 2022), що забезпечує збереження надійності сприйняття формованого стеганоповідомлення в умовах порівняно значної пропускну здатності прихованого каналу.

В роботі (Ray et al., 2021) представлено метод, заснований на глибокому навчанні: автори пропонують використовувати згорткову нейронну мережу з детектором контурів, що дозволяє їм віднайти та зберігати більшу кількість пікселів, що належать контурам, порівняно з традиційними алгоритмами виявлення контурів. Розроблену в роботі модель детектора застосовано для отримання мапи контурів. Автори стверджують, що запропонований ними метод дає змогу зберегти надійність сприйняття стеганоповідомлення у разі порівняно значної пропускну здатності прихованого каналу.

Sarrafpour et al. (2021) запропоновано стеганометод для приховування інформації в RGB-зображеннях. Тут пікселі ЦЗ-контейнера, що належать контурам, виявляються за допомогою фільтра Собеля. Саме в ці обрані пікселі (в синю складову) за допомогою LSB-методу відбувається вбудова бітів ДІ. Як стверджують автори, запропонований селективний алгоритм дозволяє уникнути спотворень ЦЗ в результаті стеганоперетворення, має незначну обчислювальну складність.

Зауважимо, що зведення результатів селекції до вибору областей контурів ЦЗ-контейнера для вбудови ДІ, хоча і з урахуванням особливостей системи людського зору, є природним для забезпечення візуальної якості отриманого стеганоповідомлення, проте не зможе забезпечити в загальному випадку якісне використання як контейнера випадкового ЦЗ, адже воно може виявитися таким, де перепади значень яскравості в межах усього зображення будуть зовсім незначними – воно може взагалі не містити контурів. За досить незначних перепадів значень яскравості методи виявлення контурів часто виявляються неспроможними виявити ці перепади. В такому випадку пропускну здатність формованого стеганографічного каналу в умовах означеної селекції прямуватиме до нуля, що є неприйнятним для прихованого каналу зв'язку.

Зазначимо, що в жодній із розглянутих вище робіт, як і в переважній більшості наявних статей, присвячених селективній стеганографії, питання синхронізації не піднімається.

Нині найпоширенішими стеганографічними методами є блокові, через багато причин, серед яких: необхідність ефективного забезпечення стійкості стеганометоду до атаки стиском, забезпечення незначної обчислювальної складності, наявність можливості розпаралелювання тощо, що не можна не враховувати в селективній стеганографії. У роботі (Saeed, 2020), наприклад, запропоновано метод, який передбачає попереднє розбиття ЦЗ-контейнера на локальні області – блоки. Метод містить три етапи: сегментація контейнера, визначення ступеня "складності" пікселів, вбудова ДІ. "Складність" пікселів розраховують на основі запропонованого критерію складності для блока. До блока застосовують фільтри високих частот, результатом чого є вісім отриманих залишкових відгуків, з урахуванням блока пікселів призначається один із дев'яти рівнів складності, на основі чого пікселі впорядковуються за пріоритетом складності від найвищого до найнижчого. Після цього виконують вбудову даних для



відповідного рівня складності. В статті зазначено, що експериментальні результати підтверджують збереження візуальної якості стеганоповідомлень.

Схема блокової селективної стеганографії з використанням текстурованих областей, зокрема країв і навколишніх пікселів, пропонується в (Laishram, & Tuithung, 2021), де блоки є результатом попереднього розбиття матриці ЦЗ-контейнера. Запропонована схема і побудований на її основі метод розглядають виключно просторову область контейнера для стеганоперетворення, динамічно обираючи для цього певний "region", причому цей вибір робиться серед пікселів в межах блока. Метод забезпечує вбудову ДІ з мінімальними викривленнями ЦЗ-контейнера в результаті стеганоперетворення навіть за значної пропускної спроможності прихованого каналу за рахунок вбудови трьох бітів ДІ в крайових пікселях із використанням мінімальної середньоквадратичної похибки: для відповідного стеганоповідомлення значення PSNR становить 61–65 dB навіть в умовах 80 % модифікованих блоків.

Зазначимо, що для розглянутих блокових селективних методів питання синхронізації теж залишилось поза увагою авторів.

В селективній стеганографії використовують велику кількість різноманітних принципів. Наприклад в роботі (Naji et al., 2020) селективний метод вибору області ЦЗ-контейнера для вбудови ДІ засновано на розумінні авторів, що особливу роль у ЦЗ відіграють людські обличчя, які, зазвичай, є фокусом зображення у випадку візуального сприйняття. Автори пропонують підхід, який асоціює в собі метод для визначення облич, результатом чого є автоматична побудова "мапи шкіри" для ЦЗ, з подальшою вбудовою ДІ в області, що не містять обличчя, методом LSB. Під автоматичною побудовою "мапи шкіри" автори розуміють визначення того, чи є на зображенні будь-які потенційні області, що містять шкіру людини, і якщо вони існують, то на ЦЗ виявляються місця їхнього розташування. Цей процес по суті є сегментацією. Виявлені області можуть включати будь-які відкриті частини людини – обличчя, плечі, руки, ноги тощо, де наявна шкіра. Хоча запропонований тут селективний метод дозволяє забезпечити значні значення PSNR, він, по-перше, спрямований на вузький клас контейнерів, адже, якщо говорити про застосування випадкового контейнера, він не обов'язково буде містити в межах своєї сцени людину; по-друге, процес організації декодування ДІ з необхідною синхронізацією тут, як і скрізь вище, ніяк не обговорюється.

Mohammed (2023) запропонував селективний метод, де як контейнер використано кольорове ЦЗ. Вибір області вбудови ДІ в межах контейнера відбувається із застосуванням градієнтно-селективних кривих Безьє, що дозволяє зберегти надійність сприйняття стеганоповідомлення навіть у разі збільшення пропускної спроможності прихованого каналу, для організації якого використовується LSB-метод.

Зауважимо, що запропоновані в розглянутих вище роботах сучасні селективні методи частіше за інші стеганометоди для безпосередньої вбудови ДІ використовують метод модифікації найменшого значущого біта, який сам по собі є таким, що забезпечує надійність сприйняття стеганоповідомлення (і значне значення PSNR) і без будь-якої селекції, що не дає можливості говорити тут про збереження хороших декларованих авторами характеристик запропонованих методів в умовах використання інших стеганоалгоритмів. На жаль, хоча нині селективний стеганографії приділяється значна увага, ця увага спрямована, як свідчать літературні джерела, на розв'язання окремих конкретних задач, які дуже часто стосуються селекції під конкретні стеганографічні методи, без отримання загальних принципів вибору, що знижує цінність наведених розробок. Очевидно, розглядаючи проблеми селективної стеганографії, можна дійти висновку, що бажанням тут є забезпечення можливості такого вибору сприятливих для вбудови ДІ областей контейнера, який не залежав би від способу і специфіки безпосереднього стеганоперетворення. Таке бажання для забезпечення надійності сприйняття стеганоповідомлення є природним і таким, що принципово реалізується, адже з урахуванням специфіки системи людського зору найменша ймовірність виникнення на ЦЗ помітних артефактів забезпечується змінами в високочастотній складовій зображення. Такий підхід застосовано нещодавно в (Kobozieva et al., 2025; Бобок, & Кобозева, 2025), де на базі ЗПАІС запропоновано методи вибору блоків ЦЗ-контейнера, отриманих шляхом стандартного розбиття його матриці, для вбудови ДІ з метою підвищення ймовірності збереження надійності сприйняття формованого стеганоповідомлення, що кількісно оцінювалося збільшенням значення PSNR, порівняно з випадковим використанням блоків. Запропоновані методи виконують ефективну селекцію блоків контейнера незалежно від використовуваного для безпосередньої вбудови ДІ стеганометоду. Основною кількісною характеристикою блока обрано нормовану відокремленість його максимального сингулярного числа. Такий критерій дав змогу значно підвищити PSNR порівняно з довільним вибором блоків, але питання організації процесу декодування тут теж залишилось не висвітленим.

Отже, на основі аналізу відкритих джерел можна зробити висновки, що сучасна селективна стеганографія має певну низку нерозв'язаних проблем, серед яких однією з основних є проблема синхронізації, без розв'язання якої жоден із запропонованих методів не може використовуватися на практиці.

Результати

З урахуванням поширеності в сучасному інформаційному середовищі блокових стеганографічних методів, увага в роботі приділяється саме селекції блоків.

Як уже зазначено, підвищення ефективності роботи довільного стеганографічного методу з випадковим контейнером може бути забезпечено шляхом використання вибору блоків матриці контейнера за певним критерієм для вбудови ДІ. Однак цей вибір блоків, а також визначення їхньої послідовності для стеганоперетворення, результат чого далі будемо називати блоковим стеганошляхом, що робиться для оригінального контейнера, є інформацією, необхідною у декодуванні ДІ приймальною стороною. Після вбудови ДІ обраний до стеганоперетворення набір і порядок блоків у стеганоповідомленні може бути порушений: якщо критерій відбору блоків є деякою його кількісною характеристикою, то після вбудови ДІ, що в загальному випадку збурить блок, ця кількісна характеристика з великою ймовірністю зміниться, що призведе до значного утруднення / неможливості виявлення цих блоків і їх безпосереднього порядку в стеганоповідомленні для декодування ДІ. Отже, маємо таку суперечність: селективна стеганографія забезпечує поліпшення якості для результату вбудови ДІ (якості стеганоповідомлення), але при



цьому призводить до значного утруднення організації процесу декодування ДІ, що залежить від синхронізації, оскільки у процесі використання селективної стеганографії в загальному випадку неможливо передбачити, яким саме буде блоковий стеганошлях для певного ЦЗ за певного кількісного критерію.

Для розв'язання проблеми синхронізації принципово можливі три шляхи:

1. Розглядати отриманий у результаті селекції блоків у контейнері блоковий стеганошлях як частину секретного ключа.

2. Для кожного блока зберігати інформацію про його задіяність / незадіяність у стеганоперетворенні та його порядок в обраній послідовності блоків у межах отриманого стеганоповідомлення за допомогою, наприклад, стеганографічної вбудови цієї інформації (далі – службової інформації) в контейнер разом із ДІ (корисною інформацією).

3. Проводити вбудову ДІ у такий спосіб, щоб визначальний параметр відбору блока (критерій селекції) залишався незмінним після стеганоперетворення, що дозволить приймальній стороні відновити стеганошлях.

Розглянемо детально кожний із цих варіантів для вибору найбільш прийняттого.

Перший спосіб у загальному випадку явно утруднює використання випадкового контейнера, для якого вибір блоків (визначення їхніх пріоритетів для вбудови ДІ) не можна визначити і передати заздалегідь як частину секретного ключа отримувачу, зокрема й коли критерієм селекції є деяка кількісна характеристика блока, що потребує обчислення у процесі вибору. Тут процес стеганоперетворення і передача частини секретного ключа отримувачу по захищеному каналу повинні відбуватися майже одночасно, що незручно, а іноді й неможливо. Крім того, наявність захищеного каналу зв'язку, що передбачається для передачі частини секретного ключа практично під час пересилання стеганоповідомлення, становить під питання доцільність організовувати прихований канал зв'язку в наявних умовах, принаймні, якщо обсяг частини секретного ключа, пов'язаної саме з результатами селекції блоків, буде порівнянний з обсягом ДІ, що є цифровим представленням секретного повідомлення.

Другий спосіб. Його реалізація передбачає додатково вбудову службової інформації в контейнер разом із корисною ДІ. Такий підхід значно зменшить обсяг корисної ДІ, що може бути передана, і для пересилання якої взагалі створювався стеганографічний канал. Справді, збурення контейнера, що можна розглядати в загальному випадку як непрямий показник величини сумарної пропускної спроможності прихованого каналу зв'язку (для передачі корисної і службової інформації), є обмеженням завдяки необхідності забезпечення надійності сприйняття отриманого стеганоповідомлення. Причому навіть незначне збільшення загального обсягу інформації, що вбудовується в контейнер, завдяки вбудові службової інформації, може призвести до значного якісного погіршення візуального сприйняття стеганоповідомлення, що умовно продемонстровано на рис. 1.



Рис. 1. Ілюстрація залежності ймовірності збереження надійності сприйняття стеганоповідомлення від пропускної спроможності прихованого каналу зв'язку

Третій спосіб. Зазначимо, що в загальному випадку принципово неможливо дати рекомендації, яким саме способом можна забезпечити незмінність визначального параметра блока після стеганоперетворення. Це вирішуватиметься для кожного параметра, визначального для селективного блокового вибору, окремо. Найчастіше таке забезпечення вимагатиме певної корекції визначального критерію у блоці після стеганоперетворення. Саме такий варіант забезпечення синхронізації в умовах селективної стеганографії, враховуючи наведене вище, автори вважають пріоритетним. Один із варіантів розглядається в цій роботі.

Нещодавно на основі теорії збурень і матричного аналізу розроблено ЗПАІС, який добре зарекомендував себе у розв'язанні задач захисту інформації (Браїловський та ін., 2021). Саме цей підхід став базовим для селективних методів, запропонованих в (Kobozieva et al., 2025; Бобок, & Кобозева, 2025), забезпечуючи їхню ефективність, а тому очевидно є доцільність використання ЗПАІС для розв'язання задач цієї роботи.

Нехай матриця F ЦЗ-контейнера розбивається стандартно на непересічні $l \times l$ -блоки. Окремий такий блок далі позначатимемо B . Результат вбудови ДІ в блок відповідно до ЗПАІС можна представити у загальному вигляді як: $B_S = B + \Delta B$, де B_S – блок стеганоповідомлення, ΔB – матриця збурення B у результаті стеганоперетворення. Матриця блока однозначно визначається повним набором параметрів – сингулярних чисел (СНЧ) і сингулярних векторів (СНВ) (Браїловський та ін., 2021), отриманих у результаті нормального сингулярного розкладання (Браїловський та ін., 2021):

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

де U, V – ортогональні матриці, стовпці яких $(u_1, u_2, \dots, u_l)$, $(v_1, v_2, \dots, v_l)$ є відповідно лівими і правими СНВ B , ліві СНВ є лексико-графічно додатними, а $\Sigma = \text{diag}(\sigma_1, \sigma_2, \dots, \sigma_l)$ – діагональна матриця СНЧ, для яких виконується співвідношення:

$$\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_l \geq 0. \quad (2)$$



Селекція блоків у (Kobozieva et al., 2025; Бобок, & Кобозєва, 2025) виконується відповідно до кількісного показника: нормованої відокремленості максимального СНЧ, що визначається згідно з формулою

$$svdgap_n(1) = \bar{\sigma}_1 - \bar{\sigma}_2, \quad (3)$$

де

$$\bar{\sigma}_i = \frac{\sigma_i}{\|\sigma\|} \quad (4)$$

– нормовані СНЧ, $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_l)$ – вектор СНЧ В, $\|\sigma\|$ – евклідова векторна норма.

Результат убудови ДІ у блок згідно із ЗПАІС можна представити у вигляді сукупності збурень СНЧ і СНВ (блоків) матриці контейнера, тобто у вигляді сукупності збурень сингулярних трійок (σ_i, u_i, v_i) , $i = 1, l$. Після вбудови ДІ значення всіх / деяких СНЧ, СНВ блока В зміняться, що в загальному випадку призведе і до зміни значення (3), навіть тоді, коли самі значення σ_1, σ_2 будуть незмінними, оскільки збуриться $\|\sigma\|$. Відповідно до обраного підходу до забезпечення синхронізації, після вбудови ДІ СНЧ блока стегаповідомлення B_S , що далі позначатимуться як

$$\sigma_1^{(S)}, \sigma_2^{(S)}, \dots, \sigma_l^{(S)}, \quad (5)$$

буде потрібно додатково змінити так, щоб залишити незмінним значення (3) для B_S :

$$\bar{\sigma}_1^{(S)} - \bar{\sigma}_2^{(S)} = \bar{\sigma}_1 - \bar{\sigma}_2 = svdgap_n(1) = P, \quad (6)$$

де $\bar{\sigma}_i^{(S)} = \frac{\sigma_i^{(S)}}{\|\sigma^{(S)}\|}$, $\sigma^{(S)} = (\sigma_1^{(S)}, \sigma_2^{(S)}, \dots, \sigma_l^{(S)})$, P – позначення, що використовується далі для зручності.

Зазначимо, що будь-які додаткові збурення для забезпечення синхронізації, виразом яких буде зміна СНЧ (5), в ідеалі не повинні торкнутися вбудованої ДІ, тобто призвести до додаткових збурень тих СНЧ, в первісних збуреннях яких міститься вбудована ДІ. В загальному випадку це гарантувати неможливо: якщо вбудова ДІ відбувається не в області сингулярного розкладання матриці, де є безпосередній контроль над тим, у збуреннях яких саме параметрів повного набору (СНЧ, СНВ) вона буде міститися, то не можна розраховувати на те, що якісь із цих параметрів не збуряться (більше чи менше) в результаті стегаперетворення. В загальному випадку маємо як формальне представлення ДІ сукупність збурень усіх СНЧ і СНВ. Це означає, що будь-яке додаткове збурення СНЧ після вбудови ДІ для забезпечення (6) може призвести до часткового спотворення вбудованої ДІ, представляючи фактично атаку проти вбудованого повідомлення. Оскільки наголос у роботі робиться на забезпеченні надійності сприйняття стегаповідомлення, то при вбудові ДІ, враховуючи наявні достатні умови такого забезпечення, отримані в межах ЗПАІС, збурені будуть сингулярні трійки, що відповідають найменшим СНЧ блока, причому з великою імовірністю $\sigma_1^{(S)} = \sigma_1$, $\sigma_2^{(S)} = \sigma_2$, а при декодуванні ДІ з блока B_S вбудовану ДІ збурення σ_1, σ_2 в собі нести не будуть. З огляду на це, забезпечення (6) пропонується робити шляхом модифікації $\sigma_1^{(S)}, \sigma_2^{(S)}$ у блоці стегаповідомлення.

Оскільки $\sigma_1^{(S)}$ відповідає перша сингулярна трійка B_S , яка несе в собі, головню, інформацію про низькочастотну складову блока, то з урахуванням вимоги забезпечення надійності сприйняття стегаповідомлення додаткові зміни $\sigma_1^{(S)}$ є небажаними. Змінам (за необхідності) для забезпечення (6) пропонується піддавати $\sigma_2^{(S)}$. Незважаючи на те, що сингулярна трійка $(\sigma_2^{(S)}, u_2^{(S)}, v_2^{(S)})$ теж може нести значний обсяг інформації як про середньо-, так і про низькочастотну складову, модифікація $\sigma_2^{(S)}$ з великою імовірністю не порушить надійність сприйняття стегаповідомлення. Справді, зміни найменших СНЧ при вбудові ДІ не можуть бути значними, оскільки самі їхні значення, а тому й відповідні відокремленості є малими, тому для встановлення (6) зміни для $\sigma_2^{(S)}$ теж будуть незначні в силу доброї обумовленості всіх складових сингулярного спектра (Браїловський та ін., 2021), що не призведе до виникнення артефактів у блоці.

Позначимо шукане значення зміненого $\sigma_2^{(S)}$ через α . Тоді для визначення α із (6) отримаємо рівняння

$$\bar{\sigma}_1^{(S)} - \frac{\alpha}{\|\sigma^{(S)}\|} = P. \quad (7)$$

У випадку евклідової векторної норми, яку найчастіше застосовують у задачах стегаграфії, співвідношення (7) матиме вигляд

$$\frac{\sigma_1^{(S)} - \alpha}{\|\sigma^{(S)}\|} = \frac{\sigma_1^{(S)} - \alpha}{\sqrt{(\sigma_1^{(S)})^2 + \alpha^2 + \dots + (\sigma_l^{(S)})^2}} = P,$$

представляючи квадратне відносно α рівняння, дискримінант якого D визначають так:

$$D = 4(\sigma_1^{(S)})^2(1 - (1 - P^2)^2) + 4P^2(1 - P^2)((\sigma_3^{(S)})^2 + \dots + (\sigma_l^{(S)})^2). \quad (8)$$

З огляду на те, що, за визначенням P , $0 \leq P \leq 1$, а, як буде показано нижче, $0 < P < 1$, значення (8) є додатним, із чого отримаємо можливі значення для α :

$$\alpha = \frac{\sigma_1^{(S)} \pm \sqrt{(\sigma_1^{(S)})^2(1 - (1 - P^2)^2) + P^2((\sigma_3^{(S)})^2 + \dots + (\sigma_l^{(S)})^2)}}{1 - P^2}, \quad (9)$$

але, враховуючи, що $\sigma_1^{(S)} \geq \alpha$, з (9) обираємо

$$\alpha = \frac{\sigma_1^{(S)} - \sqrt{(\sigma_1^{(S)})^2(1 - (1 - P^2)^2) + P^2((\sigma_3^{(S)})^2 + \dots + (\sigma_l^{(S)})^2)}}{1 - P^2}, \quad (10)$$

оскільки в іншому варіанті додавання до $\sigma_1^{(S)}$ додатного значення, а потім ділення на $1 - P^2$, для якого виконується

$$0 < 1 - P^2 < 1, \quad (11)$$

призведе до остаточного результату, що перевершує $\sigma_1^{(S)}$. Подвійна нерівність (11) є строгою. Дійсно, якщо припустити можливість того, що $0 = 1 - P^2$, тобто $P = 1$, то це означатиме з (3), що $\bar{\sigma}_1 - \bar{\sigma}_2 = \frac{\sigma_1 - \sigma_2}{\|\sigma\|} = 1$, тобто

$(\sigma_1 - \sigma_2)^2 = \sigma_1^2 + \sigma_2^2 + \dots + \sigma_l^2$, звідки маємо

$$-2\sigma_1\sigma_2 = \sigma_3^2 + \dots + \sigma_l^2. \quad (12)$$

Враховуючи, що для блоків оригінальних ЦЗ співвідношення (2) на практиці набуває вигляду (Bobok, & Kobozieva, 2024):

$$\sigma_1 \gg \sigma_2 \geq \dots \geq \sigma_l \geq 0, \quad (13)$$



із співвідношення (12) отримуємо систему

$$-\{ -2\sigma_1\sigma_2 \leq 0, \sigma_3^2 + \dots + \sigma_l^2 \geq 0, \sigma_1 \gg \sigma_2. \quad (14)$$

Система (14) має єдиний розв'язок:

$$\sigma_2 = \dots = \sigma_l = 0. \quad (15)$$

Проте, по-перше, як свідчить практичний досвід, це вкрай рідкісна ситуація для $l \times l$ -блока оригінального ЦЗ, а при $l \geq 8$ вона практично відсутня. По-друге, із співвідношення (15) слідує, що в цьому блоці практично відсутня середньо- і височастотна складові, що принципово не дасть змоги такому блоку бути задіяним у процесі стеганоперетворення в умовах селективної стеганографії з метою забезпечення надійності сприйняття стеганоповідомлення.

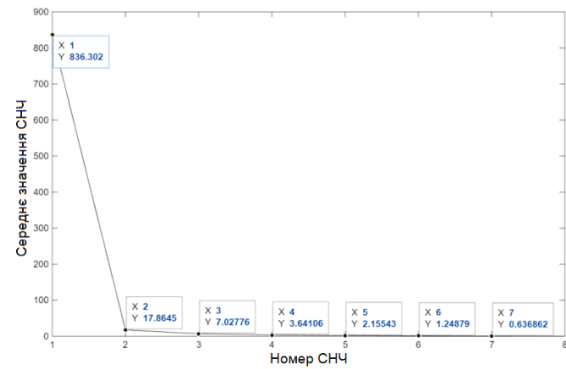
Припустимо тепер, що $1 - P^2 = 1$, тобто $P = 0$, звідки $\sigma_1 = \sigma_2$, що суперечить (13). Отже, (11) виконується.

Покажемо, що розраховане за формулою (10) $\alpha \geq \sigma_3^{(S)}$. Ця умова є важливою, оскільки при її невиконанні, якщо первісні значення $\sigma_2^{(S)}$, $\sigma_3^{(S)}$ поміняються місцями, то кількісне значення критерію селекції буде втрачене. Вбудова ДІ згідно з достатніми умовами забезпечення надійності сприйняття стеганоповідомлення буде проводитися так, щоб її результатом, головню, були збурення сингулярних трійок, що відповідають найменшим СНЧ блока, а для нас важливо – найменших СНЧ. Звісно, в загальному випадку, як зазначено вище, збурення при вбудові ДІ торкнуться (майже) всіх СНЧ блока. Враховуючи результати досліджень, наведені в (Bobok, & Kobozieva, 2025), ці збурення не можуть бути значними, оскільки основний наголос тут – на найменших СНЧ. Отже, сингулярний спектр контейнера від сингулярного спектра стеганоповідомлення буде в цілому відрізняться незначно.

Співвідношення (13) не відображає всю специфіку зменшення СНЧ у блоках ЦЗ. Зазначимо, що хоча швидкість зміни значень СНЧ залежно від номера буде максимальною у процесі переходу від першого до другого, а потім вона суттєво спадає, наближаючись до нуля для СНЧ з найбільшими номерами, ця швидкість залишиться ще значною (порівняно з останніми СНЧ) також при переході від другого до третього, наочна ілюстрація цього представлена на рис. 2. Незначні відмінності сингулярних спектрів контейнера і стеганоповідомлення призведуть до того, що додаткові збурення для $\sigma_2^{(S)}$ не можуть бути значними, а враховуючи, що відстань між другим і третім СНЧ порівняно велика, ці додаткові збурення не призведуть до зміни порядку для модифікованого $\sigma_2^{(S)}$ і $\sigma_3^{(S)}$, що повністю підтверджено результатами обчислювального експерименту.



а



б

Рис. 2. Ілюстрація типової якісної картини залежності значення СНЧ блоків ЦЗ від номера: а – оригінальне ЦЗ; б – графік залежності середніх за ЦЗ значень СНЧ блоків від номера

Отже, незалежно від стеганографічного алгоритму, що використовується для вбудови ДІ, в умовах селекції блоків контейнера, запропонований в (Kobozieva et al., 2025; Бобок, & Кобозєва, 2025), для забезпечення визначення блокового стеганошляху при декодуванні ДІ згідно із застосуванням критерієм при вбудові, рекомендується проводити модифікацію другого СНЧ блока, що задіяний в стеганоперетворенні, після вбудови ДІ відповідно до (10). Це забезпечить можливість відновлення блокового стеганошляху у разі декодування ДІ без будь-якої додаткової службової інформації.

З урахуванням усього наведеного вище, основні кроки запропонованого стеганоперетворення із забезпеченням синхронізації в умовах селекції блоків (Kobozieva et al., 2025; Бобок, & Кобозєва, 2025) виглядають так.

Крок 1. Вибір блокового стеганошляху в ЦЗ-контейнері провести відповідно до методів селекції блоків, заснованих на використанні як критерію відбору блоків нормованої відокремленості максимального сингулярного числа (Kobozieva et al., 2025; Бобок, & Кобозєва, 2025).

Крок 2. Нехай В – черговий блок контейнера, що належить блоковому стеганошляху. Для блока В:

2.1. Побудувати нормальне сингулярне розкладання (1) $B = U\Sigma V^T$.

2.2. Обчислити нормовані СНЧ (4).

2.3. Обчислити значення P нормованої відокремленості максимального СНЧ (6).

2.4. Вбудувати біт / біти ДІ довільно обраним стеганографічним алгоритмом у блок В. Результат – блок B_S , нормальне сингулярне розкладання якого: $B_S = U_S \Sigma_S V_S^T$, де $\Sigma_S = \text{diag}(\sigma_1^{(S)}, \sigma_2^{(S)}, \dots, \sigma_l^{(S)})$.

2.5. Провести корегування $\sigma_2^{(S)}$ згідно з формулою (10). Результат: $\sigma_2^{(S)k}$. Остаточна матриця СНЧ блока стеганоповідомлення: $\Sigma_{S_k} = \text{diag}(\sigma_1^{(S)}, \sigma_2^{(S)k}, \sigma_3^{(S)}, \dots, \sigma_l^{(S)})$.

2.6. Сформувати остаточний вигляд блока B_{S_k} стеганоповідомлення, що відповідає В: $B_{S_k} = U_S \Sigma_{S_k} V_S^T$.

Крок 3. Якщо вся ДІ вбудована,
то перейти на крок 4,
в іншому разі перейти на крок 2.

Крок 4. Процес стеганоперетворення завершено.



Для оцінювання ефективності запропонованого способу забезпечення можливості відновлення блокового стега-ношляху у разі декодування ДІ в умовах селекції блоків проведено обчислювальний експеримент, в якому задіяно: 300 ЦЗ з бази 4cam_auth (Hsu, & Chang, 2006) (формат Tif), 300 ЦЗ з бази img_Nikon_D70s (Gloe, & Böhme, 2010) (формат Tif), 200 ЦЗ, отриманих непрофесійними відеокамерами (формат Tif), 800 ЦЗ з бази NRCS (U.S. Department of Agriculture, 2025) (формат Jpeg). Як стеганометоди в експерименті використано: один із найстійкіших до атаки стиском стеганографічний метод (Melnik, 2012), який призводить до несистематичного виникнення арте-фактів на ЦЗ-стеганоповідомленні; один із найбільш поширених і таких, що модифікуються, методів – Коха і Жао (Конахович, Прогонов, & Пузиренко, 2018), порушення надійності сприйняття в якому може мати місце у разі збіль-шення значення параметра, що використовується при модифікації коефіцієнтів дискретного косинусного перетво-рення під час убудови біта ДІ в черговий блок. Умови проведення експерименту навмисно взято такі, які точно збігаються з умовами, що були зазначені в (Kobozieva et al., 2025). Результати експерименту наведено в табл. 1 (тут умова "Без обробки блока після стеганоперетворення" передбачає наступну передачу інформації про блоковий стеганощлях як частину секретного ключа).

Таблиця 1

Результати порівняльного оцінювання ефективності запропонованого методу синхронізації і синхронізації, що забезпечується секретним ключем

Стеганометод	Середнє по експерименту підвищення значення PSNR в умовах селекції блоків (Kobozieva et al., 2025), dB	
	Без обробки блока після стеганоперетворення (забезпечується секретним ключем)	Із запропонованою постобробкою блока
Коха і Жао (Конахович, Прогонов, & Пузиренко, 2018)	5.1	4.3
Метод (Melnik, 2012)	4.8	4.1

Зменшення значення PSNR у разі використання запропонованого в роботі методу порівняно з методом, що не передбачає додаткову обробку для відновлення кількісного значення критерію селекції, є очікуваним, оскільки, як зазначено вище, відновлення критерію призводить до додаткових, хоч і незначних, збурень. Однак цей метод є пріоритетним із погляду організації процесу декодування, оскільки не потребує збільшення обсягу секретного ключа та додаткового збереження службової інформації. Крім того, незначне погіршення PSNR ніяк не відбилося на візу-альному сприйнятті отримуваних стеганоповідомлень, що проілюстровано на рис. 3, де навмисно для порівняння використано ЦЗ з роботи (Kobozieva et al., 2025).

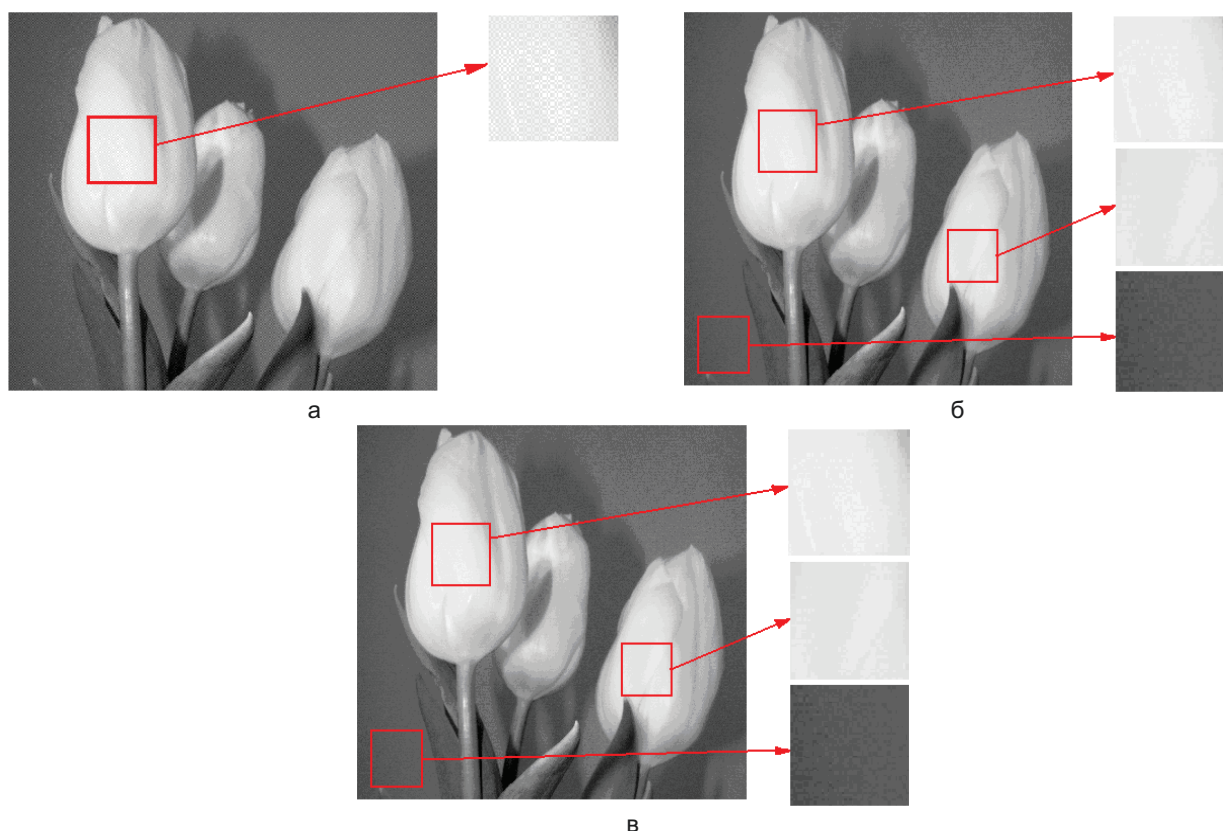


Рис. 3. Стеганоповідомлення, отримані за допомогою стеганометоду (Melnik, 2012), при формуванні яких блоки для стеганоперетворення: а – обиралися випадковим чином; б – піддавалися селекції за допомогою методу (Kobozieva et al., 2025) без подальшої будь-якої обробки; в – піддавалися селекції за методом (Kobozieva et al., 2025) із наступною обробкою запропонованим методом



Дискусія і висновки

У цій роботі розглянуто важливу науково-практичну задачу підвищення ефективності стеганографічної системи шляхом розроблення методу забезпечення синхронізації в умовах застосування селекції блоків, запропонованій у дослідженнях (Kobozieva et al., 2025; Бобок, & Кобозєва, 2025).

В ході проведеного дослідження:

- обґрунтовано доцільність обраного принципу синхронізації: забезпечення незмінності визначального параметра (критерію селекції) блока після стеганоперетворення;
- запропоновано метод, що реалізує обраний спосіб синхронізації в умовах селекції блоків, що не залежить від використовуваного стеганографічного алгоритму, заснований на модифікації другого СНЧ блока стеганоповідомлення, що належить обраному стеганошляху, з метою забезпечення незмінності нормованої відокремленості максимального сингулярного числа – кількісного критерію селекції блоків.

Застосування запропонованого механізму синхронізації в умовах селекції блоків контейнера з метою забезпечення надійності сприйняття стеганоповідомлення, дало змогу підвищити ефективність стеганосистеми на 4.1–4.3 dB, у цьому разі застосовували випадкові контейнери. І хоча такий механізм синхронізації дещо програє в ефективності тому випадку, коли вона забезпечується секретним ключем, але наявний незначний програш ніяк не впливає на якість отриманого стеганоповідомлення, про що свідчать результати обчислювального експерименту, причому обраний спосіб синхронізації не потребує розширення секретного ключа та його додаткової передачі, що одночасно робить запропонований спосіб синхронізації пріоритетним.

Перспективою подальшого дослідження є розроблення блокових селективних методів, що забезпечують стійкість результату селекції в умовах атак проти вбудованого повідомлення. Це питання до цього часу не має загальних принципів розв'язання і практично не досліджується фахівцями в цій області стеганографії.

Внесок авторів: Алла Кобозєва – концептуалізація, написання (перегляд і редагування); Світлана Григоренко – формальний аналіз, програмне забезпечення, валідація даних, написання (оригінальна чернетка).

Джерела фінансування. Це дослідження не отримало жодного гранту від фінансової установи в державному, комерційному або некомерційному секторах.

Список використаних джерел

- Бобок, І., & Кобозєва, А. (2025). Нормована відокремленість максимального сингулярного числа блоку цифрового зображення як показник доцільності його стеганоперетворення. У В. Вичужанін (Ред.), *Системи контролю інформації та інтелектуальні технології. Досягнення та застосування* (с. 58–75). Liha-Pres.
- Брайловський, М., Зибін, С., Кобозєва, А., Хорошко, В., & Хохлачова, Ю. (2021). *Аналіз кіберзахисності інформаційних систем*. ФОП "Ямчинський О. В."
- Конахович, Г., Проконов, Д., & Пузиренко, О. (2018). *Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних*. Alex Print Centre.
- Aslam, M. (2022). Image Steganography using Least Significant Bit (LSB) – A Systematic Literature Review. In *Proceedings of the 2nd International Conference on Computing and Information Technology (ICCIT'2022)* (pp. 32–38). IEEE. <https://doi.org/10.1109/ICCIT52419.2022.9711628>
- Bobok, I., & Kobozieva, A. (2024). Localization of Disturbance Region of Formal Parameters of Steganographic Cover to Ensure Steganosystem Stability. *Radioelectronics and Communications Systems*, 67, 396–409. <https://doi.org/10.20535/S0021347024090024>
- Bobok, I., & Kobozieva, A. (2025). Theoretical Foundations of Digital Content Integrity Expertise. *Problemele Energeticii Regionale*, 1, 105–121. <https://doi.org/10.52254/1857-0070.2025.1-65.08>
- Charan, S. (2023). A Review of the Recent Advances in Image Based Steganography. In *Proceedings of the KILBY 100 7th International Conference on Computing Sciences (ICCS'2023)* (pp. 1–5). Lovely Professional University. <http://dx.doi.org/10.2139/ssrn.4490256>
- Ghosal, S., Chatterjee, A., & Sarkar, R. (2021). Image steganography based on Kirsch edge detection. *Multimedia Systems*, 27, 73–87. <https://doi.org/10.1007/s00530-020-00703-3>
- 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). ACM. <https://doi.org/10.1145/1774088.1774427>
- Hsu, Y., & Chang, S. (2006). Detecting Image Splicing using Geometry Invariants and Camera Characteristics Consistency. In *Proceedings of 2006 IEEE International Conference on Multimedia and Expo* (pp. 549–552). IEEE. <https://doi.org/10.1109/ICME.2006.262447>
- Kadhim, I., Premaratne, P., & Vial, P. J. (2018). Adaptive Image Steganography Based on Edge Detection Over Dual-Tree Complex Wavelet Transform. In D. S. Huang, M. Gromiha, K. Han, & A. Hussain (Eds.), *Lecture Notes in Computer Science: Vol. 10956. Intelligent Computing Methodologies* (pp. 544–550). Springer. https://doi.org/10.1007/978-3-319-95957-3_57
- Kobozieva, A., Bobok, I., Laptiev, O., & Savchenko, V. (2025). Application of Graph Theory to Ensure the Reliability of Steganographic Message Perception in the Creation of a Covert Communication Channel. *CEUR Workshop Proceedings*, 4048, 94–108.
- Laishram, D., & Tuithung, T. (2021). A novel minimal distortion-based edge adaptive image steganography scheme using local complexity. *Multimedia Tools and Applications*, 80, 831–854. <https://doi.org/10.1007/s11042-020-09519-9>
- Melnik, M. (2012). Compression-resistant steganography algorithm. *Information Security*, 2, 99–106.
- Mohammed, S. N. (2023). Color Image Steganography Using Gradient Selective Bezier Curves. *Iraqi Journal of Science*, 64(7), 4525–4541. <https://doi.org/10.24996/ijis.2023.64.7.39>
- Naji, S., Mohaisen, H., Alsaffar, Q., & Jalab, H. (2020). Automatic region selection method to enhance image-based steganography. *Periodicals of Engineering and Natural Sciences*, 8(1), 67–78.
- Ray, B., Mukhopadhyay, S., & Hossain, S. (2021). Image steganography using deep learning based edge detection. *Multimedia Tools and Applications*, 80, 33475–33503. <https://doi.org/10.1007/s11042-021-11177-4>
- Saeed, A. (2020). An Accurate Texture Complexity Estimation for Quality-Enhanced and Secure Image Steganography. *IEEE Access*, 8, 21613–21630. <https://doi.org/10.1109/ACCESS.2020.2968217>
- Sarrafpour, B., Alomirah, R., Sarrafpour, S., & Sharifzadeh, H. (2021). An Adaptive Edge-Based Steganography Algorithm for Hiding Text into Images. In *Proceedings of the 2021 IEEE 19th International Conference on Embedded and Ubiquitous Computing (EUC)* (pp. 109–116). IEEE. <https://doi.org/10.1109/EUC53437.2021.00024>
- Taher, M., Ahmad, A. R. B. H. J., Sami, R., & Mokri, S. (2022). A literature review of various steganography methods. *Journal of Theoretical and Applied Information Technology*, 100(5), 1412–1427.
- U.S. Department of Agriculture. (2025, November 10). *NRCS Photo Gallery*. <https://www.nrcs.usda.gov>

References

- Aslam, M. (2022). Image Steganography using Least Significant Bit (LSB) – A Systematic Literature Review. In *Proceedings of the 2nd International Conference on Computing and Information Technology (ICCIT'2022)* (pp. 32–38). IEEE. <https://doi.org/10.1109/ICCIT52419.2022.9711628>
- Bobok, I., & Kobozieva, A. (2025). Normalized separability of the maximum singular number of a digital image block as an indicator of the feasibility of its steganographic transformation. In V. Vychuzhanin (Ed.), *Information control systems and intelligent technologies: Achievements and applications* (pp. 58–75). Liha-Pres [in Ukrainian].



- Bobok, I., & Kobozeva, A. (2024). Localization of Disturbance Region of Formal Parameters of Steganographic Cover to Ensure Steganosystem Stability. *Radioelectronics and Communications Systems*, 67, 396–409. <https://doi.org/10.20535/S0021347024090024>
- Bobok, I., & Kobozeva, A. (2025). Theoretical Foundations of Digital Content Integrity Expertise. *Problemele Energeticii Regionale*, 1, 105–121. <https://doi.org/10.52254/1857-0070.2025.1-65.08>
- Brailovskyi, M., Zybin, S., Kobozeva, A., Khoroshko, V., & Khokhlachova, Yu. (2021). *Analysis of cybersecurity of information systems*. FOP "Yamchynskiy O. V." [in Ukrainian].
- Charan, S. (2023). A Review of the Recent Advances in Image Based Steganography. In *Proceedings of the KILBY 100 7th International Conference on Computing Sciences (ICCS'2023)* (pp. 1–5). Lovely Professional University. <http://dx.doi.org/10.2139/ssrn.4490256>
- Ghosal, S., Chatterjee, A., & Sarkar, R. (2021). Image steganography based on Kirsch edge detection. *Multimedia Systems*, 27, 73–87. <https://doi.org/10.1007/s00530-020-00703-3>
- 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). ACM. <https://doi.org/10.1145/1774088.1774427>
- Hsu, Y., & Chang, S. (2006). Detecting Image Splicing using Geometry Invariants and Camera Characteristics Consistency. In *Proceedings of 2006 IEEE International Conference on Multimedia and Expo* (pp. 549–552). IEEE. <https://doi.org/10.1109/ICME.2006.262447>
- Kadhim, I., Premaratne, P., & Vial, P. J. (2018). Adaptive Image Steganography Based on Edge Detection Over Dual-Tree Complex Wavelet Transform. In DS. Huang, M. Gromiha, K. Han, & A. Hussain (Eds.), *Lecture Notes in Computer Science: Vol. 10956. Intelligent Computing Methodologies* (pp. 544–550). Springer. https://doi.org/10.1007/978-3-319-95957-3_57
- Kobozeva, A., Bobok, I., Laptiev, O., & Savchenko, V. (2025). Application of Graph Theory to Ensure the Reliability of Steganographic Message Perception in the Creation of a Covert Communication Channel. *CEUR Workshop Proceedings*, 4048, 94–108.
- Konakhovych, H., Prohonov, D., & Puzyrenko, O. (2018). *Computer steganographic processing and analysis of multimedia data*. Alex Print Centre [in Ukrainian].
- Laishram, D., & Tuithung, T. (2021). A novel minimal distortion-based edge adaptive image steganography scheme using local complexity. *Multimedia Tools and Applications*, 80, 831–854. <https://doi.org/10.1007/s11042-020-09519-9>
- Melnik, M. (2012). Compression-resistant steganography algorithm. *Information Security*, 2, 99–106.
- Mohammed, S. N. (2023). Color Image Steganography Using Gradient Selective Bezier Curves. *Iraqi Journal of Science*, 64(7), 4525–4541. <https://doi.org/10.24996/ijis.2023.64.7.39>
- Naji, S., Mohaisen, H., Alsaffar, Q., & Jalab, H. (2020). Automatic region selection method to enhance image-based steganography. *Periodicals of Engineering and Natural Sciences*, 8(1), 67–78.
- Ray, B., Mukhopadhyay, S., & Hossain, S. (2021). Image steganography using deep learning based edge detection. *Multimedia Tools and Applications*, 80, 33475–33503. <https://doi.org/10.1007/s11042-021-11177-4>
- Saeed, A. (2020). An Accurate Texture Complexity Estimation for Quality-Enhanced and Secure Image Steganography. *IEEE Access*, 8, 21613–21630. <https://doi.org/10.1109/ACCESS.2020.2968217>
- Sarrafpour, B., Alomirah, R., Sarrafpour, S., & Sharifzadeh, H. (2021). An Adaptive Edge-Based Steganography Algorithm for Hiding Text into Images. In *Proceedings of the 2021 IEEE 19th International Conference on Embedded and Ubiquitous Computing (EUC)* (pp. 109–116). IEEE. <https://doi.org/10.1109/EUC53437.2021.00024>
- Taher, M., Ahmad, A. R. B. H. J., Sami, R., & Mokri, S. (2022). A literature review of various steganography methods. *Journal of Theoretical and Applied Information Technology*, 100(5), 1412–1427.
- U.S. Department of Agriculture. (2025, November 10). *NRCS Photo Gallery*. <https://www.nrcs.usda.gov>

Отримано редакцією журналу / Received: 14.11.25

Прорецензовано / Revised: 17.11.25

Схвалено до друку / Accepted: 22.12.25

Alla KOBOZIEVA, DSc (Engin.), Prof.
ORCID ID: 0000-0001-7888-0499
e-mail: alla_kobozeva@ukr.net
Odesa National Maritime University, Odesa, Ukraine

Svitlana HRYHORENKO, PhD (Engin.)
ORCID ID: 0009-0006-4551-8243
e-mail: sngrygorenko@gmail.com
Odesa Polytechnic National University, Odesa, Ukraine

THE SYNCHRONIZATION PROBLEM IN SELECTIVE STEGANOGRAPHY

Background. Selective steganography is currently a powerful tool for improving the characteristics of a steganographic system, particularly when using a random container. One of the main unresolved problems of modern selective steganography remains the synchronization problem. The goal of the work is to increase the efficiency of the stego-system by ensuring synchronization under block selection, the general principles of which were proposed by the authors earlier.

Methods. The following were used: selective methods for choosing the block stego-path; a general approach to analyzing the state of information systems to study the influence of stego-transformation on container image blocks and to select the block selection criterion; perturbation theory methods for estimating the possible limits of changes in block singular values; and modern steganography methods.

Results. The feasibility of the synchronization principle was substantiated by ensuring the immutability of the determining parameter (selection criterion) of the block after stego-transformation. A method is proposed that implements the chosen synchronization approach under block selection, independent of the steganographic method used, based on modifying the block's singular spectrum to ensure the immutability of the normalized separation of the maximum singular value – a quantitative selection criterion.

Conclusions. The application of the proposed synchronization mechanism under container block selection, aimed at ensuring the reliability of stego-message perception, allowed the stego-system efficiency to be increased by 4.1–4.3 dB when using random containers. Moreover, the proposed synchronization method does not require extending the secret key and its additional transmission, nor the storage of additional information about the obtained stego-path.

Keywords: selective steganography, synchronization, digital image, singular value, random container.

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.