

**Борисенко Ірина Іванівна**

старший викладач кафедри кібербезпеки та програмного забезпечення
Національний університет «Одеська політехніка», Одеса, Україна,
ORCID: 0009-0008-1259-5888
borisenko.i.i@op.edu.ua

Якименко Ігор Зіновійович

д.т.н., доцент, декан факультету комп'ютерних інформаційних технологій
Західноукраїнський національний університет, Тернопіль, Україна
ORCID: 0000-0003-2586-6196
iyakymenko@ukr.net, jiz@wunu.edu.ua

**КРИПТОСТЕГАНОГРАФІЧНИЙ МЕТОД ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ
КОМБІНАТОРНИМИ МЕТОДАМИ**

Анотація. У роботі представлено метод дворівневого захисту інформації, який поєднує в собі криптографічний та стеганографічний підходи для забезпечення підвищеного рівня захисту конфіденційності та цілісності інформації, що передається відкритими каналами зв'язку. Шифрування перетворює інформацію у спотворений вигляд і при відкритій передачі може визвати підозру до природності її походження, більш того, криптографія в ряді країн заборонена. Камуфлювання зашифрованих даних всередині медіа контейнері не визиває підозр при його відкритій пересилці або зберіганні. Одночасне використання криптографічного і стеганографічного методів в одному програмному рішенні вимагає узгодженості між ними, тому запропоновано підхід, в якому і для шифрування і для вбудовування інформації в контейнер використовується один і той самий метод, а саме метод транспозиції (перестановки). Основну увагу приділено приховуванню конфіденційних даних у цифрових зображеннях (хоча не порушується загальність міркувань і для інших медіа контейнерів) із забезпеченням високої стійкості до статистичних атак за рахунок того, що елементи не корегуються, а переставляються. Розроблений метод забезпечує високу надійність відновлення конфіденційної інформації, та простоту алгоритмічної реалізації.

Ключові слова: стеганографія, криптографія, контейнер, перестановки

ВСТУП

Сучасний етап розвитку суспільства характеризується стрімким поширенням інформаційних технологій, їх інтенсивним удосконаленням та масштабним впровадженням у практично всі сфери людської діяльності. Цифровізація виробничих, управлінських, фінансових, комунікаційних та соціальних процесів зумовлює постійне зростання обсягів інформації, що створюється, передається, опрацьовується та зберігається в інформаційно-комунікаційних системах. Водночас розширення функціональних можливостей і підвищення складності таких систем супроводжується зростанням кількості потенційних вразливостей та посиленням загроз несанкціонованого доступу, модифікації, перехоплення й знищення інформації. За таких умов особливої актуальності набуває завдання забезпечення належного рівня інформаційної та кібербезпеки, що передбачає розроблення й удосконалення ефективних методів і засобів захисту інформації від сучасних та перспективних кіберзагроз [1].

На сьогодні, системи захисту інформації є комплексними [2] і повинні враховувати специфіку функціонування інформаційної системи, яку вони захищають. Для формування основних програмних елементів систем захисту інформації сьогодні існують два основні напрямки [3]: стеганографія і криптографія.

Завдяки методам стеганографії приховується сам факт передавання інформації. Таким чином, конфіденційність даних забезпечується завдяки тому, що зловмисникам складно її виявити. Водночас криптографічні методи дозволяють приховати зміст даних.

Обидва напрямки зазнали суттєвого розвитку, в результаті чого кожний з них вніс суттєвий вклад для вирішення того чи іншого завдання у практично реалізованих комплексних системах захисту інформації. Тим не менш, поєднання цих підходів дозволяє побудувати багатошаровий захист інформації



більш ефективний з точки зору надійності. Так, спочатку зломиснику потрібно виявити факт передавання даних, а потім розкрити їх зміст, шляхом розшифрування.

ПОСТАНОВКА ПРОБЛЕМИ.

Основним завданням стегоаналізу є виявлення ознак наявності прихованого повідомлення у стегоконтейнері [4]. Водночас сучасні методи стегоаналізу не обмежуються лише встановленням факту прихованої передачі інформації. Окремий клас стегоаналітичних атак спрямований на локалізацію, вилучення та, за можливості, відновлення змісту прихованого повідомлення зі стегоконтейнера [5, 6], що суттєво розширює спектр завдань і методів сучасного стегоаналізу.

Природним шляхом підвищення ефективності захисту інформації, прихованої в зображенні, є застосування методів криптографії. Оскільки, у випадку, коли стегоаналітику навіть вдасться вилучити дані із стегоконтейнера, розшифрувати інформацію без знання ключа за певний час буде складно.

Наразі відомі і розробляються нові підходи до поєднання стеганографічних методів захисту з криптографічними. Однак ці підходи передбачають використання різних контейнерів, різних стеганографічних та різних криптографічних алгоритмів – все це залишається поза увагою детального дослідження ступеня взаємодії цих складових. При цьому вибір певних алгоритмів може як покращувати показники якості захисту інформації, так їх і погіршувати. Внаслідок цього постає актуальна задача вибору таких стего та крипто алгоритмів, які б узгоджувалися між собою, та побудови методу захисту інформації на основі визначеної найкращої комбінації.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ.

Огляд сучасних джерел показав, що методика поєднання методів стеганографії та криптографії достатньо поширена в наукових колах і досліджується у ряді робіт.

Так в роботі [7] пропонується дворівнева гібридна система безпеки для захисту конфіденційних даних у мережах Інтернет речей (IoT). Автори використовують комбінацію криптографічного алгоритму AES та методів стеганографії 3D-DWT і LSB. Ефективність запропонованого гібридного підходу (AES + 3D-DWT + LSB) у дослідженні оцінюється за трьома основними критеріями: непомітність (якість зображення), стійкість до атак та криптографічний захист. PSNR – понад 30–40 дБ, низьке значення MSE, використання AES гарантує, що навіть у разі виявлення стеганографічного контейнера, зломисник не зможе прочитати вміст без секретного ключа. Разом з тим метод має суттєві недоліки, такі як високий час виконання через багатоетапну обробку та обмежена ємність контейнера. Слід зазначити, що даний підхід вразливий до спотворень та стиснення, що робить його неефективним в умовах нестабільних IoT-мереж. В [8] представлена чотирирівнева схема для забезпечення конфіденційності і цілісності даних в хмарних середовищах. Криптографічна частина представлена алгоритмами: AES-256 – для швидкого та надійного шифрування даних користувача, RSA – для шифрування та безпечної передачі сесійних ключів AES між користувачами, хеш-функцією (зокрема SHA-256) – для генерації цифрових відбитків даних з метою перевірки їхньої цілісності та виявлення модифікацій. Інструмент стеганографії – LSB. Динамічна чотириетапна модель захисту даних, попри високу конфіденційність, характеризується високими обчислювальними витратами через багаторівневу обробку та вразливістю методу LSB до модифікацій файлів. Додатковими недоліками є складність управління ключами, обмежена місткість стегоконтейнерів та неможливість пошуку зашифрованих даних у хмарі. У дослідженні [9] пропонується дворівнева система захисту, яка перетворює конфіденційні дані за допомогою математичних операцій та приховує їх усередині іншого файлу, роблячи передачу інформації практично непомітною для перехоплювачів. Етап шифрування – система використовує DWT, отримані компоненти потім обробляються математично за допомогою експоненціальних функцій для повного спотворення інформації; етап стеганографії – DWT з використанням вейвлета Добеші (db1); далі – у структурі матриці контейнера-зображення виділяються конкретні координати, які математично зануляються, на місце цих занулених позицій записуються зашифровані (за допомогою експоненціальної функції) коефіцієнти секретного зображення. Недоліки представленої схеми: висока обчислювальна складність (потреба в ресурсах – DWT/IDWT, особливо для 3D-зображень) вимагає значних потужностей процесора; використання експоненціальних функцій на великих матрицях коефіцієнтів уповільнює процес кодування та декодування у реальному часі; обмежена місткість приховування (дефіцит позицій – робота у частотній області (DWT) суттєво обмежує кількість доступних коефіцієнтів, які можна занулити й замінити без критичного руйнування структури зображення, співвідношення розмірів – контейнер має бути в рази більшим за розміром та роздільною здатністю, ніж секретне повідомлення, щоб приховування залишалося непомітним); чутливість до алгоритмів стиснення із втратами; вразливість до статистичного стегоаналізу; ризик повної втрати зв'язку через одну помилку.



В роботі [10] для шифрування використовується блоковий симетричний шифр AES в режимі роботи OFB, ключ шифрування приєднується до зашифрованих даних, а вбудовування в зображення відбувається методом кластеризації найближчого центроїда. Основним недоліком такого підходу є зберігання ключа шифрування разом з даними, які зашифровані цим ключем з подальшою їх пересилкою в одному контейнері. Таким чином, шифрування дозволило авторам покращити статистичні властивості зашифрованої інформації для ускладнення виконання криптоаналізу. Однак при цьому, застосування криптографії не утворило ще один рівень захисту, оскільки при успішному стегоаналізі розшифрувати дані не становитиме складності, оскільки зловмиснику буде доступним ключ шифрування. В роботі [11] автори пропонують шифрування та подвійне використання стеганографічного перетворення. Отже, спочатку відкритий текст зашифровують, потім вбудовують в один контейнер, який вбудовують в інший контейнер. Автори вважають, що внаслідок успішного стегоаналізу зловмисником буде виявлено дані, які насправді є контейнером для приховування справжнього секрету. Відповідно зловмисник зупинить подальший аналіз, отримавши контейнер. Автори не зазначають використовувані криптографічні перетворення та спосіб передачі ключа. Більше того вони пропонують використання методу LSB для вбудовування даних в зображення, який є нестійким для будь-якого виду атак. В роботі [12] наведено детальний аналіз крипто-стеганографічних методів, автори відзначають відсутність оцінок стійкості результату поєднання криптографічного та стеганографічного методів. Навіть у тих випадках, коли відбувається аналіз отриманих результатів, то він виконується методами стегоаналізу, ігноруючи криптографічні складові запропонованих методів. В роботі [13] автори розглядають поєднання LSB з DES, Blowfish та дискретним косинусним перетворенням. Комбінація алгоритмів DES, Blowfish, DCT та LSB створює гібридну систему з екстремальним рівнем безпеки: стійкість до атак та стиснення (властивість DCT), висока швидкість та стійкість до зламу (властивість Blowfish), візуальна непомітність (властивість LSB). Попри високу безпеку, комбінація DES, Blowfish, DCT та LSB має серйозні технічні компроміси. Поєднання просторових і частотних методів створює технологічні конфлікти, які формують наступні недоліки: конфлікт архітектур (DCT проти LSB), критичне обмеження місткості – DCT вимагає розбиття зображення на блоки 8x8 пікселів і дозволяє ховати дані лише в обмежену кількість середньочастотних коефіцієнтів (можна сховати лише 1–5% даних від загального розміру контейнера), низька обчислювальна швидкість, вразливість DES та надлишковість шифрування, вразливість до статистичного стегоаналізу (RS-атаки). В [14] в якості криптографічного алгоритму автори обрали AES, а стеганографічного – Convolutional Neural Networks (CNN). Запропоновано ввести критерії вибору криптографічних перетворень таким чином, щоб їх поєднання разом зі стеганографічними давали найкращий ефект. Визначені параметри адаптивного шифрування та вибору контейнера. До ключових недоліків методу слід віднести: висока обчислювальна складність, процес адаптивного аналізу контейнера та динамічної зміни алгоритмів уповільнює передачу даних у реальному часі, вразливість до руйнування контейнера, сучасні методи статистичного стегоаналізу можуть виявити аномалії у розподілі бітів файлу, що виявить сам факт приховування, ускладнена синхронізація ключами (відправник і отримувач повинні мати синхронізовані ключі як для дешифрування, так і для визначення адаптивного алгоритму вилучення).

Отже, з огляду на проведений аналіз сучасних джерел, криптографічна складова критостеганографічних методів в основному базується на підстановочно-перестановочних алгоритмах, які достатньо розповсюджені на сьогоднішній день. Ці алгоритми зарекомендували себе як надійні криптостійкі шифри, які забезпечують швидкість роботи та універсальність реалізації – від смартфонів до військових систем. Саме тому, наприклад, AES став міжнародним золотим стандартом шифрування і використовується практично всюди.

Однак це не означає, що розробки в напрямку криптошифрування повинні припинитися.

Попри багато переваг AES має низку недоліків [15,16,17]: фіксований розмір блоку, а це означає, що дані меншого розміру треба доповнювати (padding), а великі – розбивати на блоки (неправильне використання padding може призвести до padding oracle атак); детермінізм без режимів (якщо зашифрувати однаковий текст тим самим ключем, результат буде однаковим, це робить AES у «чистому вигляді» небезпечним, для захисту потрібні режими роботи: CBC, CTR, GCM); вразливість до побічних атак – хоча математично AES стійкий, його реалізації можуть бути атаковані (Таймінг-атаки (аналіз часу виконання), Power analysis (споживання енергії), Cache атаки (взаємодія з кешем CPU), ЕМ-атаки (електромагнітні випромінювання), а це особливо небезпечно для смарт-карт, IoT-пристроїв, вбудованих систем; управління ключами – найчастіше AES «ламають» не через криптоаналіз, а через погане управління ключами (збереження ключів поруч із даними, використання «жорстко прописаних» ключів у коді, відсутність ротації ключів).

Стосовно криптосистеми DES, вразливості якої були виявлені ще у 1991 році і висвітлені в роботі [18], а подальший аналіз стійкості цієї криптосистеми дозволив виявити низку ефективних атак [19].



Мета статті. Метою роботи є розробка комбінованого методу подвійної транспозиції елементів повідомлення і контейнера, як криптографічної та стеганографічної складової для забезпечення ефективного захисту конфіденційної інформації з точки зору надійності сприйняття стегоповідомлення без спотворення його статистичних характеристик.

Для досягнення мети необхідно розв'язати наступні задачі:

1. Проаналізувати сучасні підходи, техніки, методики одночасного використання методів криптографії та стеганографії для захисту конфіденційної інформації.
2. Розробити метод шифрування вихідного повідомлення.
3. Побудувати алгоритм вбудовування зашифрованих даних в контейнер.
4. Побудувати алгоритмічну структуру комбінованого крипто-стеганографічного метода захисту конфіденційної інформації.
5. Провести оцінку стійкості до статистичних атак та візуальної непомітності розробленого програмного рішення.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Ключовим, фундаментальним аспектом побудови комбінованого алгоритму на основі методів транспозиції є формалізація та розв'язання специфічних алгебраїчних рівнянь, базовими елементами яких виступають не звичайні числа, а математичні абстракції – перестановки.

Перестановкою будемо називати бієкцію φ скінченної множини M на себе [20]. Отже, φ є перестановка на M тоді і тільки тоді, коли для довільних елементів $a, b \in M$, $a \neq b$ маємо $\varphi(a) \neq \varphi(b)$. А це означає, що перестановка визначається таблицею виду:

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ a_1 & a_2 & a_3 & \dots & a_n \end{pmatrix} \quad (1)$$

де $a_1, a_2, \dots, a_n$ – різні елементи з множини M . Обернена перестановка визначається кроками: $\varphi' = \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ 1 & 2 & 3 & \dots & n \end{pmatrix} \rightarrow \varphi^{-1} = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ a'_1 & a'_2 & a'_3 & \dots & a'_n \end{pmatrix}$

Правило 1. Щоб побудувати перестановку обернену даній φ^{-1} треба поміняти рядки перестановки φ місцями, а потім стовпці переставити так, щоб числа першого рядка були розміщені у зростаючому порядку, другий рядок – шукана перестановка (зауважимо, що є і інші способи знаходження φ^{-1} [20]).

Наприклад, $\varphi = (5 \ 9 \ 1 \ 8 \ 2 \ 6 \ 4 \ 7 \ 3)$, представляємо φ у матричному вигляді і поміняємо рядки місцями $\varphi' = \begin{pmatrix} 5 & 9 & 1 & 8 & 2 & 6 & 4 & 7 & 3 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix}$, після упорядкування стовпців по першому рядку одержуємо остаточно $\varphi^{-1} = (3 \ 5 \ 9 \ 7 \ 1 \ 6 \ 8 \ 4 \ 2)$.

Для будь-яких перестановок визначена операція добутку. Операція добутку перестановок визначена згідно правил композиції відображень. Наприклад, для перестановок $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}$ і $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ добуток (композиція) має вигляд $\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$, тобто спочатку виконується відображення τ , а потім σ . Зауважимо, що $\sigma \circ \tau \neq \tau \circ \sigma$, $\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$, тобто множення перестановок некомутативна операція.

Перестановки (1) утворюють групу, яка називається симетричною групою n -го порядку і позначається S_n . Використовуючи основні поняття комбінаторики, можна довести важливу теорему.

Теорема 1. Порядок $|S_n|$ групи S_n дорівнює $n!$ [20].

На основі математичного апарату, розглянутому вище, проєктується комплексний підхід для розробки крипто-стеганографічного методу з робочою назвою `double _ Permut`.

Слід підкреслити, що `double _ Permut` буде базуватися на синтезі двох різних наукових напрямків: методів просторового приховування даних (галузь цифрової стеганографії) та шифрування в галузі криптографії в групі симетричних перестановок. Основна, концепція стеганографічного підходу полягає не в модифікації або перезапису значень кольору самих пікселів, а у зміні їхнього взаємного просторового розташування виключно всередині локальних, закритих блоків. Такий підхід дозволить зберегти загальну глобальну гістограму цифрового зображення абсолютно незмінною, тим самим одержаний стегоконтейнер буде стійким до більшості методів сучасних аналітичних систем та сканерів статистичного стегоаналізу.

Моделювання криптографічних примітивів та створення нових шифрів у скінченних групах перестановок практично завжди зводиться до розв'язання фундаментального рівняння наступного виду:

$$P \times K = B, \quad (2)$$



де P – код символу секретного повідомлення або відкритий, немодифікований вихідний блок даних, представлений перестановкою;
 K – наперед відома (для легітимних сторін взаємодії) перестановка, що виступає в ролі секретного симетричного ключа;
 B – результуюча, кінцева перестановка, яку отримуємо на виході (це може бути зашифрований блок даних, або просторово перемішаний мікро-блок пікселів, тобто шифрограма).
 Рівняння (2) має розв'язок відносно P , і він єдиний [21], який може бути визначений за такою формулою:

$$P = B \times K^{-1} \quad (3)$$

При шифруванні повідомлення (криптографічна складова) буде використовуватися деякий допоміжний масив *masPermut* («літера-перестановка»), в якому знаходиться k перестановок довжини n . Всі перестановки пронумеровані. При шифруванні елемента повідомлення з кодом i в масиві *masPermut* необхідно знайти перестановку P з номером i , помножити її на ключ K за формулою (2), в результаті чого одержимо перестановку B .

Вбудовування зашифрованого елемента повідомлення (стегаграфічна складова) відбувається шляхом перестановки пікселів блоку контейнера згідно одержаної перестановки B , причому тільки в тому випадку, якщо для будь-якої пари елементів, які обмінюються місцями, різниця їх значень не перевищує деяке значення d .

Розглянемо на числовому прикладі описаний сценарій.

Поставимо кожній букві українського алфавіту у відповідність перестановку з 5 цифр (масив *masPermut*): $A \rightarrow (1,2,3,4,5)$, $Б \rightarrow (1\ 2\ 3\ 5\ 4)$, $В \rightarrow (1\ 2\ 4\ 3\ 5)$ і так до літери $Я \rightarrow (2\ 3\ 4\ 1\ 5)$.

У якості ключа візьмемо перестановку K , яка не відповідає жодній літері алфавіту, такі «вільні» перестановки є, оскільки $5!=120$ (теорема 1), а літер українського алфавіту – 33.

Для визначеності, візьмемо $K=(5,3,1,4,2)$. Знайдемо для K обернену їй перестановку $K^{-1}=(3,5,2,4,1)$ (правило 1).

Зашифруємо перші 5 літер слова «ПЕРЕМОГА». Скористаємося формулою (2), одержимо:

- 1) $П \rightarrow P_П=(1,5,2,4,3)$ $B_П=(1,5,2,4,3) \times (5,3,1,4,2)=(5,2,3,4,1)$;
- 2) $Е \rightarrow P_Е=(1,2,5,4,3)$ $B_Е=(1,2,5,4,3) \times (5,3,1,4,2)=(5,3,2,4,1)$;
- 3) $Р \rightarrow P_Р=(1,5,3,2,4)$ $B_Р=(1,5,3,2,4) \times (5,3,1,4,2)=(5,2,1,3,4)$;
- 4) $М \rightarrow P_М=(5,4,3,2,1)$ $B_М=(5,4,3,2,1) \times (5,3,1,4,2)=(2,4,1,3,5)$.

Кожну літеру i будемо вбудовувати шляхом перестановки пікселів контейнера відповідно до її зашифрованої перестановки B_i , використовуючи оператор перестановки:

$$S(P(j))=C(j), \quad (4)$$

де C – контейнер, S – стего.

Наприклад, щоб вбудувати літеру «Р», якій в таблиці перестановок відповідає перестановка $(1,5,3,2,4)$, а її зашифрованою версією є $B_Р=(5,2,1,3,4)$, треба виконати перестановку пікселів блоку контейнера C відповідно до $B_Р$. Нехай блок контейнера має такі значення пікселів $C=[120,125,130,135,140]$ відповідно до $B_Р$ одержимо стегоблок $S=[130,125,135,140,120]$. Таким способом вбудовується кожна літера у відповідний блок контейнера.

На етапі вбудовування може виникнути ситуація, коли $C_n - C_m > d$, d – це межа, яку не можна «переступати», інакше на стегоконтейнері з'являться артефакти; в цьому випадку блок пропускається. Для зображень-контейнерів емпірично встановлюється значення d , при яких зорова система людини не відрізняє контейнер від стегоконтейнера.

Запропонований алгоритм належить до класу несліпих стеганографічних алгоритмів, оскільки для коректного вилучення прихованого повідомлення на приймальній стороні необхідна наявність не лише отриманого стегоконтейнера, а й вихідного контейнера, що використовувався на етапі вбудовування інформації.

За умови, якщо значення C і S відомі, існує можливість відновлення перестановки, застосованої для формування S на основі вихідного значення C .

Перестановка P задає відображення $S(P(j))=C(j)$, де $P(j)$ – позиція елемента $C(j)$ в S . Таким чином, відновлення перестановки можна формально описати оператором:

$$P(j)=\text{poss}(C(j)), \quad (5)$$



де $\text{poss}(x)$ повертає індекс елемента x в стежоконтейнері S .

Застосувавши формулу (5) одержимо перестановку (5,2,1,3,4), яка була використана на етапі вбудовування. Відповідно до формули (3) визначається перестановка, яка відповідає символу прихованого повідомлення: $(5,2,1,3,4) \times (3,5,2,4,1) = (1,5,3,2,4)$. Отримана перестановка (1,5,3,2,4) зіставляється з елементами таблиці відповідності «літера – перестановка», представленої масивом *masPermut*. У результаті встановлюється, що зазначений перестановці відповідає літера «Р». Аналогічна процедура послідовно виконується для кожного наступного елемента стежоконтейнера, що забезпечує поетапне відновлення всіх символів прихованого повідомлення.

Алгоритмічна структура методу *double_Permut*, в загальному вигляді представляється наступними кроками.

Процедура вбудовування повідомлення

Вхід: зображення-контейнер (матриця C), повідомлення M .

Крок 1. Створити масив *masPermut* («літера→перестановка») по визначеному правилу, усі рядки занумерувати; вибрати ключ K (перестановка з *masPermut*, яка не призначена жодній літері алфавіту); визначити d для зображення, яке буде використовуватися як контейнер.

Крок 2. Для поточної літери повідомлення з кодом i знайти відповідну їй перестановку P_i в *masPermut*; застосувати формулу (2) – результат B_i .

Крок 3. Матрицю контейнера-зображення C розбити на блоки C_r розміру 1×5 .

Крок 4. Виконати перестановку елементів блоку C_r у відповідності до перестановки B_i , використовуючи (4), якщо:

– для будь-якої пари (m, h) блоку контейнера C_r виконується умова $|C_{rm} - C_{rh}| \leq d$;

– інакше в $K_{\text{блок}}$ записати номер C_r і перейти до наступного блоку.

Вихід: стежоконтейнер S , контейнер C , ключ K , $K_{\text{блок}}$.

Процедура відновлення повідомлення

Вхід: стежоконтейнер S , контейнер C , ключ K , $K_{\text{блок}}$.

Крок 1. Створити масив *masPermut* («літера→перестановка») тим самим способом, що і на етапі вбудовування.

Крок 2. Розбити матрицю контейнера C та стежоконтейнера S на блоки 1×5 .

Крок 3. Відповідно до ключа $K_{\text{блок}}$ знайти блок, в який була вбудована поточна літера повідомлення, порівняти блоки контейнера C_i та стежоконтейнера S_j , використовуючи (5), та визначити перестановку B_i .

Крок 4. Обчислити перестановку P_i , згідно формули (3).

Крок 5. Перестановку P_i знайти в масиві *masPermut*; порядковий номер i , який відповідає P_i , є кодом літери, вбудованої у блок повідомлення.

Вихід: повідомлення M .

АНАЛІЗ СТІЙКОСТІ КРИПТОГРАФІЧНОЇ СКЛАДОВОЇ МЕТОДА DOUBLE_PERMUT

При створенні масиву *masPermut* кількість можливих призначень перестановок із групи S_5 для українського алфавіту дорівнює $N = \binom{120}{33} \cdot 33!$ (комбінаторна конфігурація «розміщення»). Це означає, що існує велика кількість різних схем кодування букв українського алфавіту. Приблизну оцінку числа N можна дати формулою Стерлінга $k! \approx \left(\frac{k}{e}\right)^k \sqrt{2\pi k}$. В результаті отримується неймовірно велике число, приблизно порядку 10^{66} .

Тобто, якщо перестановки вибираються псевдовипадково на основі ключа (псевдовипадковий генератор на ключі), то таблиця «літера → перестановка» стає секретним словником і без знання ключа відновлення повідомлення не є тривіальною задачею, навіть маючи контейнер і стего.

Далі необхідно врахувати, що ключову перестановку K можна вибрати з 87 перестановок, які не призначені жодній літері алфавіту. Це збільшить криптостійкість шифру, а саме: збільшується простір ключів – кількість можливих схем «літера → перестановка» множиться на 87; підвищується складність відновлення – відновити початкову таблицю стає значно важче, оскільки потрібно одночасно відгадати ключ і призначення; з'являється ефект «маскування» – ключова перестановка діє як «змішувач» – вона руйнує пряму відповідність між літерою і перестановкою, що додає рівень секретності, схожий на використання гамування у класичних шифрах.

Якщо дозволити використовувати кілька ключових перестановок m із 87 вільних і застосовувати їх послідовно (тобто брати добутки кілька разів), то криптостійкість системи ще більше зростає. Детальніше: якщо взяти m ключових перестановок із 87, це експоненційно збільшує простір ключів (при



$m=4$ і більше простір ключів стає настільки великим, що перебір вручну чи простим скриптом практично неможливий); складність атаки – тепер зломиснику потрібно не лише відновити таблицю відповідностей «літера → перестановка», а й розкрити послідовність ключових перестановок. Це перетворює задачу на розв'язання рівнянь у симетричній групі S_5 , що значно складніше, ніж простий частотний аналіз; створюється додаткова дифузія – кожне множення ключової перестановки «перемішує» структуру ще більше, що нагадує багатораундові шифри (як у AES, DES), де кожен раунд додає плутанину й дифузію.

Таким чином, формула для N приймає вигляд – $N' = \binom{120}{33} \cdot 33! \cdot 87^m$. Неважко помітити, що кількість можливих ключових комбінацій N' різко зростає при збільшенні послідовності ключів m : при $m=1$ – близько 10^{77} , при $m=2$ – близько 10^{79} , при $m=3$ – близько 10^{81} .

Це наочно демонструє, що навіть невелике збільшення послідовності ключів m дає колосальний приріст у стійкості криптосистеми.

Можна дати оцінку складності перебору ключів, наприклад, скільки часу займе *brute-force* при сучасних швидкостях обчислень. Припустимо, що суперкомп'ютер може перевіряти 10^{12} ключів за секунду (1 трильон операцій/с), тоді $T = \frac{N'}{10^{12}} = 10^{69}$ секунд, а якщо перевести в роки, то $\approx 3.2 \cdot 10^{61}$ років, навіть найпотужніші сучасні системи не здатні перебрати такий простір ключів.

Але простір ключів можна ще збільшити, враховуючи некомутативність операції добутку перестановок, тобто $\sigma \circ \tau \neq \tau \circ \sigma$. Це означає, що для послідовності з m ключів кожен порядок перестановок дає різний результат. Тобто отримується додатковий множник у просторі ключів, який враховує всі можливі перестановочні порядки. Отже, враховуючи некомутативність, потрібно помножити ще на кількість перестановок ключової послідовності m : $N_{\text{заг}} = \binom{120}{33} \cdot 33! \cdot 87^m \cdot m!$.

Таким чином, врахування некомутативності добутку перестановок робить криптографічну складову ще стійкішою: простір ключів росте не лише експоненційно від m , а й факторіально від порядку перестановок.

АНАЛІЗ СТЕГАНОГРАФІЧНОЇ СКЛАДОВОЇ МЕТОДА DOUBLE_PERMUT

Поріг візуальної непомітності d обмежує можливість перестановки занадто контрастних пікселів.

Інтуїтивно ясно, що щоб не з'являлися артефакти на зображенні, при перестановці двох пікселів, їхні яскравості (інтенсивності) повинні якнайменше відрізнятися одна від одної і тим паче, їхня різниця не повинна перевищувати поріг d .

У зв'язку з цим вибір зображення є важливим з точки зору його текстурної деталізації. Серед характеристик текстури [22] корисними для перестановочної стеганографії будуть однорідність та ентропія. Велика однорідність означає, що сусідні пікселі мають близькі значення. Якщо такі пікселі переставити місцями, локальна структура не порушується, і зміни залишаються непомітними. Низька ентропія (0-3) свідчить про те, що розподіл інтенсивності більш передбачуваний і рівномірний. На таких ділянках складніше виявити приховані зміни статистичними методами, бо вони не створюють різких відхилень.

Отже, гладкі зображення (наприклад, зображення поля, неба, моря, рівні поверхні) – ідеальні для перестановок, оскільки мають високу однорідність і низьку ентропію.

Вибір гладкого зображення в якості контейнера дозволить збільшити об'єм вбудовування за рахунок того, що кількість пропущених блоків буде мінімальною.

ОЦІНКА ЕФЕКТИВНОСТІ ЗАПРОПОНОВАНОГО МЕТОДУ DOUBLE_PERMUT

Простір ключів дуже і дуже великий, що робить перебір неможливим, атакуючий не може спростити добутки перестановок і звести до єдиної «еквівалентної» перестановки, оскільки порядок множення має значення. І криптографія (ключові перестановки), і стеганографія (гладкі блоки з порогом $d \leq 10$) базуються на перестановках, що створює багаторівневу стійкість, де криптографічна стійкість зростає експоненційно, а непомітність забезпечується адаптивним вибором блоків контейнера.

На рис.1 видно, що для класичного Permutation ентропія зростає помірно зі збільшенням довжини ключа m .

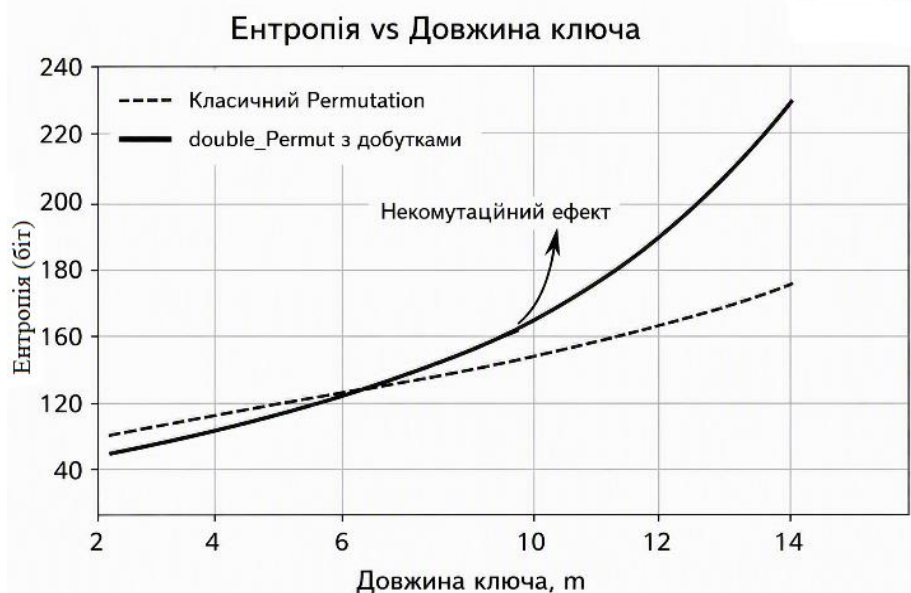


Рис.1. Залежність ентропії від довжини ключа

А для методу double_Permut з добутками крива різко піднімається вгору саме завдяки ефекту некомутативності.

Це означає, що при малих m різниця ще не дуже велика, але вже при $m \geq 8$ ентропія методу double_Permut значно перевищує класичний варіант, при $m=14$ вона стає майже вдвічі більшою, що робить перебір абсолютно нереалістичним. Таким чином, запропонований підхід не просто розширює простір ключів, а створює експоненційний приріст стійкості завдяки некомутативності добуток перестановок.

Перевірка стійкості до статистичного стегааналізу проводилась за двома тестами:

χ^2 -тест перевіряє, чи зміни у гістограмі пікселів відрізняються від природного розподілу. У методі double_Permut перестановка не змінює значення пікселів у контейнері, а лише змінює їхній порядок. Оскільки перестановка виконується лише у гладких блоках ($d \leq 10$), то локальні статистики залишаються майже незмінними. Подвійна перестановка (крипто + стего) ще більше «розмиває» закономірності, але без порушення розподілу. Отже, χ^2 -значення залишається близьким до природного і це забезпечує високу стійкість. Для практичних контейнерів визначено відхилення $\chi^2 < 0.05$, тобто атака не має статистично значущих ознак.

RS-аналіз шукає різницю між групами пікселів (Regular/Singular) після інверсії. У double_Permut перестановка не змінює парність чи інверсію пікселів, тому RS-тест не знаходить різниці між групами. Некомутативні добуток перестановок створюють нерегулярну структуру блоків, що руйнує кореляцію між сусідніми групами. Адаптивний поріг ($d \leq 10$) гарантує, що перестановка не зачіпає контрастні області, де RS-аналіз найефективніший. Якщо RS-показники ($R-S$ різниця) прямують до нуля, то забезпечується висока стійкість. Для гладких контейнерів $|R-S| < 1\%$, що нижче порогу виявлення.

Для прикладу на рис.2(а) представлено стегоконтейнер, побудований на основі гладкого зображення, та його статистичний стегааналіз – рис.2 (б). Зауважимо, що ніяких артефактів на стего немає і не може бути, враховуючи метод, за яким ми його одержали.

Ліворуч рис.2 (б) – χ^2 -аналіз: видно, що при невеликій кількості прихованих бітів статистика лишається низькою, а лише після 2000 бітів починає перевищувати поріг виявлення. Це підтверджує високу стійкість стегоконтейнера до класичних χ^2 -атак.

Праворуч рис.2 (б) – RS-аналіз: різниця $|R-S|$ тримається в межах «зони стійкості» ($< 1-1,5\%$) аж до великих навантажень. Це означає, що перестановки у гладких блоках добре маскують дані й не створюють помітних аномалій для RS-тестів.

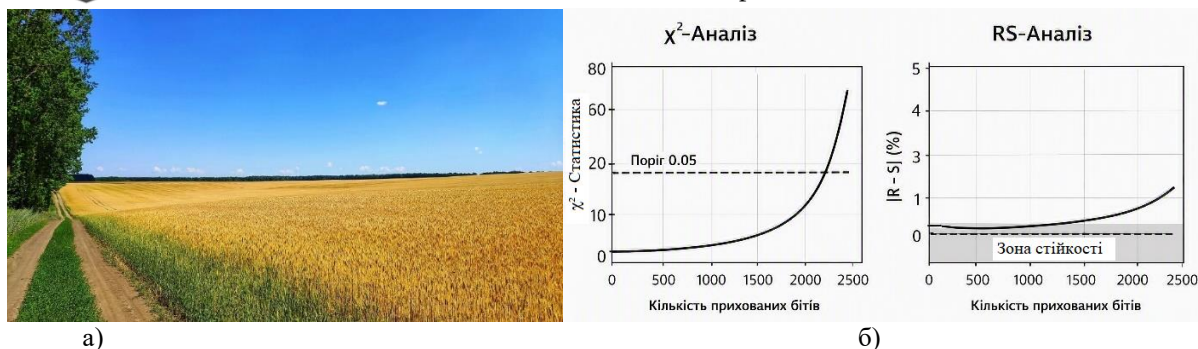


Рис.2. Стегоконтейнер (а) і його статистичний стегааналіз (б)

Можна зробити висновок, що `double_Permut` для цього стегаконтейнера демонструє високу стійкість одночасно до χ^2 - та RS-аналізу, особливо при середніх обсягах приховування, подібна ситуація і для інших зображень, що досліджувалися.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

В роботі запропоновано новий крипто-стегаграфічний метод `double_Permut`, в якому перестановки застосовуються не тільки до пікселів контейнера, а також і до повідомлення, що вбудовується. Досліджено і проаналізовано переваги, які дає попереднє шифрування повідомлення на базі перестановок.

Детально проаналізовано можливості і запропоновано напрямки збільшення простору ключів криптографічної складової (при $m=3$ – близько 10^{81}). Здійснена оцінка складності перебору ключів, що дозволяє стверджувати про майже абсолютну криптостійкість. Враховуючи некомутативність добутку перестановок простір ключів росте не лише експоненційно від m , а й факторіально від порядку перестановок, що ще збільшує криптостійкість.

За результатами аналізу стегаграфічної складової встановлено, що найбільш придатними для вбудовування прихованих повідомлень у межах досліджуваного методу є цифрові зображення, які характеризуються однорідною текстурою та незначними локальними змінами яскравості. Для представленого зображення на рис.2 (а), перед вбудовуванням, були обчислені кількісні характеристики його синього каналу – однорідність і ентропія. Однорідність $\sim 0.92 \rightarrow$ синій канал має високий ступінь регулярності: велика частина кадру (небо) складається з близьких за інтенсивністю пікселів. Ентропія ~ 6.8 біт $\rightarrow$ розподіл синіх значень досить різноманітний, але не максимальний (8 біт). Це означає, що є як однорідні області (небо), так і контрастні (дерева, трава). Синя складова поєднує високу однорідність у великих блоках та помірну ентропію через наявність контрастних деталей. Це робить її придатною для стегаграфічного приховування – гладкі ділянки маскують зміни, а різноманітність розподілу ускладнює статистичний аналіз.

Побудовані графіки аналізу статистичних атак на стегаконтейнери, виявлені діапазони об'єму вбудованої інформації, для яких χ^2 -аналіз і RS-тести не дають позитивного результату, що є показником високої статистичної стійкості `double_Permut`.

До переваг запропонованого методу слід віднести простоту математичного апарату, узгодженість криптографічної і стегаграфічної складової – єдиною базою є симетричні групи перестановок.

Представлена структура крипто-стегаграфічного методу `double_Permut` гарантує двохфакторний захист даних, що відповідає концепції "Defense in Depth". Навіть у тому малоімовірному випадку, якщо досвідчений зловмисник знайде спосіб виявити сам факт перестановки пікселів (наприклад, отримавши доступ до оригінального фотографічного знімка та порівнявши його з перехопленим стегаконтейнером) він математично отримає лише фінальну перестановку B_i . Проте без фізичного володіння секретними ключами, які зберігаються лише у відправника та отримувача, він принципово не зможе відновити повідомлення.

Криптографічна складова запропонованого методу становить окремий науковий інтерес з погляду дослідження криптографічних перетворень у симетричних групах. Водночас її використання як самостійного криптографічного методу потребує подальшого теоретичного та експериментального обґрунтування, зокрема дослідження стійкості до відомих класів криптоаналітичних атак, оцінювання алгебраїчної стійкості та визначення параметрів, що характеризують рівень криптографічної безпеки. Разом із тим інтеграція зазначеної криптографічної складової у метод `double_Permut` забезпечує



формування додаткового рівня захисту прихованої інформації та підвищує складність її несанкціонованого відновлення.

Перспективи подальших досліджень полягають у поглибленому аналізі криптографічної та стеганографічної стійкості методу double_Permut, дослідженні його стійкості до сучасних методів крипто- та стегоаналізу, а також визначенні оптимальних параметрів вбудовування. Окремим напрямом є порівняльна оцінка запропонованого методу з відомими криптостеганографічними рішеннями за показниками стійкості, швидкодії та обсягу прихованої інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Vakulyk O. et al. Cybersecurity as a component of the national security of the state. *Journal of Security & Sustainability Issues*. 2020. Vol. 9, No. 3. P. 775-784. [https://doi.org/10.9770/jssi.2020.9.3\(4\)](https://doi.org/10.9770/jssi.2020.9.3(4))
2. Хорошко В. О. та ін. Проектування комплексних систем захисту інформації. Видавництво Львівської політехніки, 2020. 317 с.
3. Mohammed M. H. Analysis on Contribution of Cryptography and Steganography in Protecting Information in Diverse Environments. *Proceedings of Third International Conference on Communication, Computing and Electronics Systems*. Singapore: Springer, 2022. P. 153-158. https://doi.org/10.1007/978-981-16-8862-1_11
4. Чистов В.І. та ін. Дослідження статистичних методів стегоаналізу цифрових зображень. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України*. 2023. №. 1(77). С. 130-135.
5. Римар П. В., Крохмалюк В. В. Атаки на стеганосистеми. Криптографічні атаки. *Матеріали наукової конференції професорсько-викладацького складу, наукових працівників і здобувачів наукового ступеня за підсумками науково-дослідної роботи за період 2019–2020 рр. (квітень–травень 2021 р.)*. ДонНУ ім. Василя Стуса Вінниця. 2021. С. 344-346.
6. Лагун А.Е. Атаки на сучасні стеганографічні системи і методи захисту. *Вісник ЛДУ БЖД*. 2016. №.13. С. 6-12.
7. Sangeetha R., Koteeswari G., Phil M. Securing Data in IOT using Cryptography & Steganography Techniques. *Int. J. Res. Eng. Sci.* 2021. Vol. 9. P. 1-5.
8. Adeel R., Mouratidis H. A Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography. *Sensors*. 2022. Vol. 22. No. 3. P. 1109. <https://doi.org/10.3390/s22031109>
9. ALRikabi H. T. H. S., Hazim H. T. Enhanced data security of communication system using combined encryption and steganography. *ijim*. 2021. Vol. 15, No. 16. P. 145. <https://doi.org/10.3991/ijim.v15i16.24557>
10. Shifa A. et al. Joint Cryp to-Stego Scheme for Enhanced Image Protection With Nearest-Centroid Clustering. *IEEE Access*. 2018. Vol. 6. P. 16189-16206 DOI:10.1109/ACCESS.2018.2815037
11. 16206.Bandela H. B. et al. Crypto-Stego Technique for Secure Data Transmission. *Journal of Physics: Conference Series*. 1228, 012012. 2019. P. 11. <https://doi.org/10.1088/1742-6596/1228/1/012012>
12. Jan A. et al. Double layer security using crypto-stego techniques: comprehensive review. *Health and Technology*. 2021. Vol.12. P. 9–31. <https://doi.org/10.1007/s12553-021-00602-1>
13. Singhal, V., Singh, D., Gupta S. K., (2022). Crypto STEGO Techniques to Secure Data Storage Using DES, DCT, Blowfish and LSB Encryption Algorithms. *Journal of Algebraic Statistics*. 2022. Vol. 13, No. 3. P. 1162-1171.
14. Лукічов В. В. та ін. Метод адаптивного багатoshарового захисту інформації на основі стеганографії і криптографії. *Інформаційні технології та комп'ютерна інженерія*. 2023. №3. С.4-11.
15. What are the limits of AES? (2025). https://hub.sivo.it.com/cryptographic-algorithm-limitations/what-are-the-limits-of-aes/?utm_source=copilot.com (дата звернення: 18.07.2026).
16. AES-256 Encryption: 6 Critical Security Gaps Exposed (2025). https://www.kiteworks.com/secure-file-sharing/encryption-security-gaps/?utm_source=copilot.com (дата звернення: 18.07.2026).
17. Advantages and Disadvantages of AES (2025). https://hub.sivo.it.com/cryptography-standard/what-are-the-advantages-and-disadvantages-of-aes/?utm_source=copilot.com (дата звернення: 18.07.2026).
18. Biham, E., Shamir, A. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*. 1991. Vol.4.P. 3–72. <https://doi.org/10.1007/BF00630563>
19. Biham E. & Perle S. Conditional Linear Cryptanalysis - Cryptanalysis of DES with Less Than 2^{42} Complexity. *IACR Transactions on Symmetric Cryptology*. 2018. No. 3. P. 215-264. DOI:10.13154/tosc.v2018.i3.215-264



20. Стасюк М. Елементи математичних основ криптографії : навч.-метод. посіб. Львів : ЛДУ БЖД, 2021. 216 с.
21. Борисенко І.І., Кас'яненко М.М. Математичні методи комбінаторики як засіб створення криптографічних шифрів. *Збірник матеріалів НПК молодих вчених, аспірантів та студентів «Кібербезпека та комп'ютерно-інтегровані технології»(КБКІТ – серпень, 2025).* Тернопіль. 2025. С. 99-102.
22. Gonzalez R. C., Woods R. E. Digital Image Processing. 4th ed. New York : Pearson, 2018. 1192 p

**Iryna I. Borysenko**

Senior Lecturer at the Department of Cybersecurity and Software
Odesa Polytechnic National University, Odesa, Ukraine
ORCID: 0009-0008-1259-5888
borisenko.i.i@op.edu.ua

Ihor Z. Yakymenko

Doctor of Technical Sciences, Associate Professor, Dean of the Faculty of Computer Information Technologies
West Ukrainian National University, Ternopil, Ukraine
ORCID: 0000-0003-2586-6196
iyakymenko@ukr.net, jiz@wunu.edu.ua

**A CRYPTOSTEGANOGRAPHIC METHOD FOR PROTECTING CONFIDENTIAL INFORMATION
USING COMBINATORIAL METHODS**

Abstract. The paper presents a two-level information protection method that combines cryptographic and steganographic approaches to provide an enhanced level of confidentiality and integrity protection for information transmitted over open communication channels. Encryption transforms information into an unintelligible form and, when transmitted openly, may raise suspicions about the nature of its origin; moreover, cryptography is prohibited in a number of countries. Camouflaging encrypted data within a media container does not raise suspicion during its open transmission or storage. The simultaneous use of cryptographic and steganographic methods within a single software solution requires consistency between them; therefore, an approach is proposed in which the same method, namely the transposition (permutation) method, is used both for encryption and for embedding information into a container. Particular attention is paid to hiding confidential data in digital images, although the generality of the approach is also preserved for other types of media containers. High resistance to statistical attacks is achieved because the elements are not modified but rearranged. The developed method provides high reliability in recovering confidential information and is characterized by simplicity of algorithmic implementation.

Keywords: steganography, cryptography, container, permutations.

REFERENCES

1. Vakulyk O. et al. Cybersecurity as a Component of the National Security of the State. *Journal of Security & Sustainability Issues*. 2020. Vol. 9, No. 3. P. 775–784. DOI: 10.9770/jssi.2020.9.3(4).
2. Khoroshko V. O. et al. *Design of Integrated Information Security Systems*. Lviv: Lviv Polytechnic Publishing House, 2020. 317 p. [in Ukrainian].
3. Mohammed M. H. Analysis on Contribution of Cryptography and Steganography in Protecting Information in Diverse Environments. *Proceedings of the Third International Conference on Communication, Computing and Electronics Systems*. Singapore: Springer, 2022. P. 153–158. DOI: 10.1007/978-981-16-8862-1_11.
4. Chystov V. I. et al. Research on Statistical Methods of Steganalysis of Digital Images. *Collection of Scientific Papers of the Center for Military and Strategic Studies of the National Defence University of Ukraine*. 2023. No. 1(77). P. 130–135. [in Ukrainian].
5. Rymar P. V., Krokhamliuk V. V. Attacks on Steganographic Systems. Cryptographic Attacks. *Proceedings of the Scientific Conference of Faculty Members, Researchers and Degree Candidates Based on the Results of Research Work for 2019–2020 (April–May 2021)*. Vasyl Stus Donetsk National University. Vinnytsia, 2021. P. 344–346. [in Ukrainian].
6. Lagun A. E. Attacks on Modern Steganographic Systems and Protection Methods. *Bulletin of Lviv State University of Life Safety*. 2016. No. 13. P. 6–12. [in Ukrainian].
7. Sangeetha R., Koteeswari G., Phil M. Securing Data in IoT Using Cryptography & Steganography Techniques. *International Journal of Research in Engineering and Science*. 2021. Vol. 9. P. 1–5.
8. Adeel R., Mouratidis H. A Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography. *Sensors*. 2022. Vol. 22, No. 3. Art. 1109. DOI: 10.3390/s22031109.
9. AlRikabi H. T. H. S., Hazim H. T. Enhanced Data Security of Communication System Using Combined Encryption and Steganography. *International Journal of Interactive Mobile Technologies (IJIM)*. 2021. Vol. 15, No. 16. P. 145. DOI: 10.3991/ijim.v15i16.24557.



10. Shifa A. et al. Joint Crypto-Stego Scheme for Enhanced Image Protection With Nearest-Centroid Clustering. *IEEE Access*. 2018. Vol. 6. P. 16189–16206. DOI: 10.1109/ACCESS.2018.2815037.
11. Bandela H. B. et al. Crypto-Stego Technique for Secure Data Transmission. *Journal of Physics: Conference Series*. 2019. Vol. 1228. Art. 012012. DOI: 10.1088/1742-6596/1228/1/012012.
12. Jan A. et al. Double Layer Security Using Crypto-Stego Techniques: Comprehensive Review. *Health and Technology*. 2022. Vol. 12. P. 9–31. DOI: 10.1007/s12553-021-00602-1.
13. Singhal V., Singh D., Gupta S. K. Crypto STEGO Techniques to Secure Data Storage Using DES, DCT, Blowfish and LSB Encryption Algorithms. *Journal of Algebraic Statistics*. 2022. Vol. 13, No. 3. P. 1162–1171.
14. Lukichov V. V. et al. Adaptive Multilayer Information Protection Method Based on Steganography and Cryptography. *Information Technology and Computer Engineering*. 2023. No. 3. P. 4–11. [in Ukrainian].
15. What Are the Limits of AES? 2025. Available at: <https://hub.sivo.it.com/cryptographic-algorithm-limitations/what-are-the-limits-of-aes/> (accessed: 18 July 2026).
16. AES-256 Encryption: 6 Critical Security Gaps Exposed. 2025. Available at: <https://www.kiteworks.com/secure-file-sharing/encryption-security-gaps/> (accessed: 18 July 2026).
17. Advantages and Disadvantages of AES. 2025. Available at: <https://hub.sivo.it.com/cryptography-standard/what-are-the-advantages-and-disadvantages-of-aes/> (accessed: 18 July 2026).
18. Biham E., Shamir A. Differential Cryptanalysis of DES-like Cryptosystems. *Journal of Cryptology*. 1991. Vol. 4. P. 3–72. DOI: 10.1007/BF00630563.
19. Biham E., Perle S. Conditional Linear Cryptanalysis – Cryptanalysis of DES with Less Than 2^{42} Complexity. *IACR Transactions on Symmetric Cryptology*. 2018. No. 3. P. 215–264. DOI: 10.13154/tosc.v2018.i3.215-264.
20. Stasiuk M. *Elements of the Mathematical Foundations of Cryptography: Study and Methodological Manual*. Lviv: Lviv State University of Life Safety, 2021. 216 p. [in Ukrainian].
21. Borysenko I. I., Kasianenko M. M. Mathematical Methods of Combinatorics as a Tool for Creating Cryptographic Ciphers. *Proceedings of the Scientific and Practical Conference of Young Scientists, Postgraduate Students and Students “Cybersecurity and Computer-Integrated Technologies” (CBCIT – August 2025)*. Ternopil, 2025. P. 99–102. [in Ukrainian].
22. Gonzalez R. C., Woods R. E. *Digital Image Processing*. 4th ed. New York: Pearson, 2018. 1192 p.

Отримано редакцією журналу / Received: 14.06.26

Прорецензовано / Revised: 28.07.26

Схвалено до друку / Accepted: 26.10.26



This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.