

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
Навчально-науковий фізико-технічний інститут
Кафедра математичних методів захисту інформації

«На правах рукопису»

УДК 044.056.55

«До захисту допущено»

Завідувач кафедри

_____ Сергій ЯКОВЛЄВ

«__» _____ 2026 р.

Дипломна робота
на здобуття ступеня бакалавра
за освітньо-професійною програмою
«Математичні методи криптографічного захисту інформації»

зі спеціальності: 113 Прикладна математика
на тему: **«Розробка та аналіз малоресурсного алгоритму
захисту відеопотоків з властивістю нерозповсюдження
помилки»**

Виконав:

студент IV курсу, групи ФІ-23

Безнощенко Марія Андріївна _____

Керівник:

д.т.н., проф. каф. ММЗІ

Ковальчук Людмила Василівна _____

Рецензент:

посада, степінь, звання

Прізвище Ім'я По-батькові _____

Засвідчую, що у цій дипломній
роботі немає запозичень з праць
інших авторів без відповідних
посилань.

Студент _____

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»

Навчально-науковий фізико-технічний інститут
Кафедра математичних методів захисту інформації

Рівень вищої освіти — перший (бакалаврський)
Спеціальність — 113 Прикладна математика,
ОПП «Математичні методи криптографічного захисту інформації»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Сергій ЯКОВЛЄВ

«__» _____ 2026 р.

ЗАВДАННЯ
на дипломну роботу

Студент: Безнощенко Марія Андріївна

1. Тема роботи: *«Розробка та аналіз малоресурсного алгоритму захисту відеопотоків з властивістю нерозповсюдження помилки»*,
науковий керівник дисертації: д.т.н., проф. каф. ММЗІ Ковальчук
Людмила Василівна,

затверджені наказом по університету №__ від «__» _____ 2026 р.

2. Термін подання студентом роботи: «__» _____ 2026 р.

3. Об'єкт дослідження: процес шифрування відеопотоку БпЛА

4. Предмет дослідження: малоресурсні алгоритми шифрування
відеопотоку з властивістю нерозповсюдження помилки

5. Перелік завдань:

1) провести огляд опублікованих джерел за темою дослідження;
2) розробити малоресурсний алгоритм захисту відеопотоків, який би
забезпечував властивість нерозповсюдження помилки;

3) проаналізувати запропонований алгоритм й оцінити його час
роботи, пам'ять та стійкість до атак перебору.

6. Орієнтовний перелік графічного (ілюстративного) матеріалу:
Презентація доповіді

7. Орієнтовний перелік публікацій: планується доповідь на всеукраїнській конференції

8. Дата видачі завдання: 10 вересня 2025 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання	Примітка
1	Узгодження теми роботи із науковим керівником	01-15 вересня 2025 р.	Виконано
2	Огляд опублікованих джерел за тематикою дослідження	Вересень-жовтень 2025 р.	Виконано
3	Ознайомлення з малоресурсними алгоритмами шифрування відеопотоку	Жовтень-грудень 2025 р.	Виконано
4	Формулювання вимог для майбутнього алгоритму шифрування	Січень-лютий 2025 р.	Виконано
5	Розробка алгоритму шифрування з властивістю нерозповсюдження помилки	Березень-квітень 2025 р.	Виконано
6	Аналіз розробленого алгоритму шифрування з властивістю нерозповсюдження помилки	Травень 2025 р.	Виконано
7	Оформлення результатів дипломної роботи	Червень 2025 р.	Виконано

Студент _____ Марія БЕЗНОЩЕНКО

Керівник _____ Людмила КОВАЛЬЧУК

РЕФЕРАТ

Кваліфікаційна робота містить: 27 стор., 1 рисунок, 13 джерел.

Метою дослідження є розробка малоресурсних алгоритмів для шифрування відеопотоків. Об'єктом дослідження є процес шифрування відеопотоку БПЛА. Предметом дослідження є малоресурсні алгоритми шифрування відеопотоку з властивістю нерозповсюдження помилки.

У ході дослідження було запропоновано малоресурсний алгоритм шифрування відеопотоку з властивістю нерозповсюдження помилки. В представлений моделі було проведено оцінку ключового простору, покращення для реалізації, оцінено обсяг потрібної пам'яті та час роботи, проаналізовано стійкість до атаки перебору та деяких інших атак.

МАЛОРЕСУРСНА КРИПТОГРАФІЯ, ШИФРУВАННЯ
ВІДЕОПОТОКУ, БПЛА, ВЛАСТИВІСТЬ НЕРОЗПОВСЮДЖЕННЯ
ПОМИЛКИ

ABSTRACT

The qualification work contains: 27 pages, 1 figures, 13 citations.

Research objective is to develop lightweight algorithms for video stream encryption. Research object is process of UAV video stream encryption. Research subject is lightweight video stream encryption algorithms with the error non-propagation property.

During the research, a lightweight video stream encryption algorithm with error non-propagation property was proposed. For the presented model, the key space was evaluated and implementation improvements were developed, the required memory consumption and execution time were estimated, the resistance to brute-force attacks and several other attacks was analyzed.

LIGHTWEIGHT CRYPTOGRAPHY, VIDEO STREAM
ENCRYPTION, UAVS, ERROR NON-PROPAGATION PROPERTY

ЗМІСТ

Вступ.....	7
1 Огляд літератури	9
Висновки до розділу 1.....	11
2 Блокові PRESENT-подібні шифри.....	13
Висновки до розділу 2.....	14
3 Малоресурсний алгоритм з властивістю нерозповсюдження помилки .	16
Висновки до розділу 3.....	23
Висновки	25
Перелік посилань	26

ВСТУП

Актуальність дослідження. Через стрімкий розвиток у використанні безпілотних літальних апаратів в усіх галузях, актуальність захисту даних, що передаються, особливо для видів пристроїв, які мають обмежені технічні характеристики, полягає в представленні алгоритмів, щоб мали достатню стійкість та потрібну малoresурсність. Багато пропонованих способів шифрування для відеопотоків, що передаються не ідеальним каналом, не враховують розповсюдження помилки, що є критичним для деяких видів БпЛА. Зокрема через вплив на керування.

Метою дослідження є розробка малoresурсних алгоритмів для шифрування відеопотоків. Для досягнення мети необхідно розв'язати **задачу дослідження**, тобто розробити та проаналізувати алгоритм шифрування відеопотоку з властивістю нерозповсюдження помилки. Для розв'язання задачі необхідно вирішити такі завдання:

- 1) провести огляд опублікованих джерел за темою дослідження;
- 2) розробити малoresурсний алгоритм захисту відеопотоків, який би забезпечував нерозповсюдження помилки;
- 3) проаналізувати запропонований алгоритм й оцінити його час роботи, пам'ять та стійкість до атак перебору.

Об'єктом дослідження є процес шифрування відеопотоку.

Предметом дослідження є малoresурсні алгоритми шифрування відеопотоку з властивістю нерозповсюдження помилки.

При розв'язанні поставлених завдань використовувались такі *методи дослідження*: методи прикладної алгебри, методи комбінаторики, методи криптографії.

Наукова новизна отриманих результатів полягає у розробленні нового алгоритму тимчасової стійкості, який не розповсюджує помилку. Що робить його орієнтованим саме на використання в роботі БпЛА.

Практичне значення результатів полягає у можливості

використанні їх реалізації, а саме запропонованого алгоритму шифрування відеопотоків в умовах неідеального каналу зв'язку, з додатковими урахуваннями щодо подачі зображення та технічними обмеженнями згаданих пристроїв.

1 ОГЛЯД ЛІТЕРАТУРИ

В першому розділі оглядається література за темою. Це і та, що присвячена основним питанням безпеки, які виникають при використанні БпЛА, і та, що — огляду можливих рішень шифрування даних та відеопотоку серед: малоресурсних алгоритмів, алгоритмів побудованих на різних перестановках й відображеннях.

Безпілотні літальні апарати (БпЛА) різного виду сьогодні застосовуються в абсолютно різних галузях, починаючи з сільського господарства і закінчуючи військовою справою. Ефективне та якісне шифрування відеопотоку є однією з важливих цілей забезпечення безпеки такого обладнання, адже для деяких пристроїв, наприклад для дронів типу FPV, затримки є досить критичними для управління.

Робота 2025 року [1] детально описує проблеми та загрози безпеці даних, що можуть виникати при роботі з БпЛА. Автори поділяють їх на апаратні, комунікаційні та програмні. Зокрема це і атака людина посередині, і перехоплення незашифрованих даних, і захоплення керування, і DoS атаки. Крім того, звертається увага на механізми криптографічного захисту каналів та обмеженні можливості, ресурси подібних пристроїв. Робота більш зосереджена на піднятті технічних питань безпеки в поєднанні з їх нормативно-правовими аспектами.

Огляд ж [2] класифікує роботи станом на 2025 рік вже саме зосереджуючись на малоресурсних алгоритмах, механізмах керування ключами, постквантовій криптографії для БпЛА. Серед малоресурсних блокових шифрів, згадують, як ті, що можуть бути найбільш пристосованими для використання на практиці, — PRESENT, SPECK, SIMON, а серед поточкових — Trivium та Grain. Зокрема зазначається, що крім криптографічної стійкості слід звертати увагу на затримку в роботі алгоритмів, енергоспоживання, неідеальні умови польоту та стану каналу передачі даних.

Автори роботи [3] оглядають наявні методи шифрування зображень, що побудовані на основі відображень Арнольда, побітових методах, хаотичних перетвореннях, перестановок. Виділяються гібридні хаотично-квантові та перестановки з розсіюванням, через майже ідеальні показники ентропії та великі ключові простори. Проте такі представники є занадто ресурсоемними для використання в реальному часі для більшості БПЛА. Малоресурсні побітові та алгоритми перестановки є кращими варіантами. Згадується також, що деякі БПЛА малого й середнього розміру використовують процесори ARM Cortex-A57 або NVIDIA Jetson із частотою 1–2.5 ГГц та обсягом оперативної пам'яті 2–8 ГБ. Відповідно до чого наголошується потреба у виборі методів, що забезпечують компроміс між ресурсоемністю та криптостійкістю.

Серед алгоритмів шифрування зображень, що не змінюють значення самих пікселів, досить поширене використання, вже раніше згаданого, відображення Арнольда. Запропонована схема в [4] насамперед будується таким чином та використовує афінний шифр для змін самих значень. Піксель поділяється на 8 біт, де кожен біт змінює позицію за допомогою відображення. Автори стверджують достатню стійкість до перебору ключів, але без детальних пояснень. Результати аналізу показують покращені статистичні показники на відміну від алгоритмів, що використовують лише перестановки. Використання такого способу шифрування для відеопотоків не обговорюється роботою, але будова виглядає як доволі ресурсоемна конструкція для реалізації в реальному часі.

Модифіковане відображення Арнольда пропонується та аналізується в [5]. Автори зауважують, що новий підхід збільшує кількість ключів та стійкість до атаки перебору. А зміна обмежень на матриці дозволяє виконувати перестановки для довільних розмірів. Що, наприклад робить алгоритм більш придатним для можливого використання при шифруванні кадру відеопотоку.

Робота [6] розглядає використання БПЛА для військових потреб, й

саме для варіантів передачі зображень на великі відстані й у високій якості. За запропонованою моделлю стверджується можливість передачі даних в реальному часі. Автори пропонують алгоритм шифрування відеопотоку побудований на кодуванні *Fibonacci-p*. Оцінки показують покращення результатів в порівнянні з наявними схожими алгоритмами. Через що також зауважується, що використання лише перестановок в більшості випадків є не достатнім для стійкості алгоритмів шифрування зображень до статистичних атак.

Автори ж в [7] пропонують малоресурсний алгоритм шифрування на основі ChaCha20-Poly1305 та стенографії. Запропонований підхід шифрування був практично випробуваний на обладнанні схожому до того, що використовується в БпЛА. А саме це Pixhawk 2.4.8. з 32-бітним STM32F427 Cortex-M4 процесором, 256KB RAM та 2MB флешпам'яттю. Крім того як бортовий комп'ютер використовується Raspberry Pi 3 Model B+ з Broadcom BCM2837B0 процесором, що є чотириядерним Cortex-A53 (ARMv8) 64-бітним SoC, та з SD пам'яттю 1GB LPDDR2. З результатів, наприклад час шифрування для 100 байтів складає 1.201 мс, а для розшифрування 0.118 мс. Що краще ніж для AES та 3DES на тому ж обладнанні.

Робота [8] пропонує й описує метод побітового шифрування відеопотоку в реальному часі без використання розсіювання, що має зменшувати розповсюдження помилки в пакеті даних. Час шифрування складає 24.84 мс, але для набагато потужнішого обладнання ніж могло б використовуватися в БпЛА.

Висновки до розділу 1

З огляду літератури можемо сказати, що є велика кількість різних методів шифрування відеопотоків та зображення, частина з яких є або занадто ресурсоємними, або не має достатньо певного виду аналізу, щоб точно сказати чи можлива їх модифікація для використання в

малоресурсних пристроях згаданого виду. Для багатьох методів захисту даних залишається відкритим питання нерозповсюдження помилки та роботи в реальному часі. Непогано виглядає підхід використання малоресурсних перестановок, з мінімальним обсягом додаткових обчислень, які б могли задовольнити вимоги до безпеки та швидкості роботи.

2 БЛОКОВІ PRESENT-ПОДІБНІ ШИФРИ

В цьому розділі розглядаються результати аналізу двох шифрів подібних до малоресурсного алгоритму PRESENT, а саме L16-PRESENT [9] та DONATION [10].

Структура PRESENT наведена на рисунку 2.1.

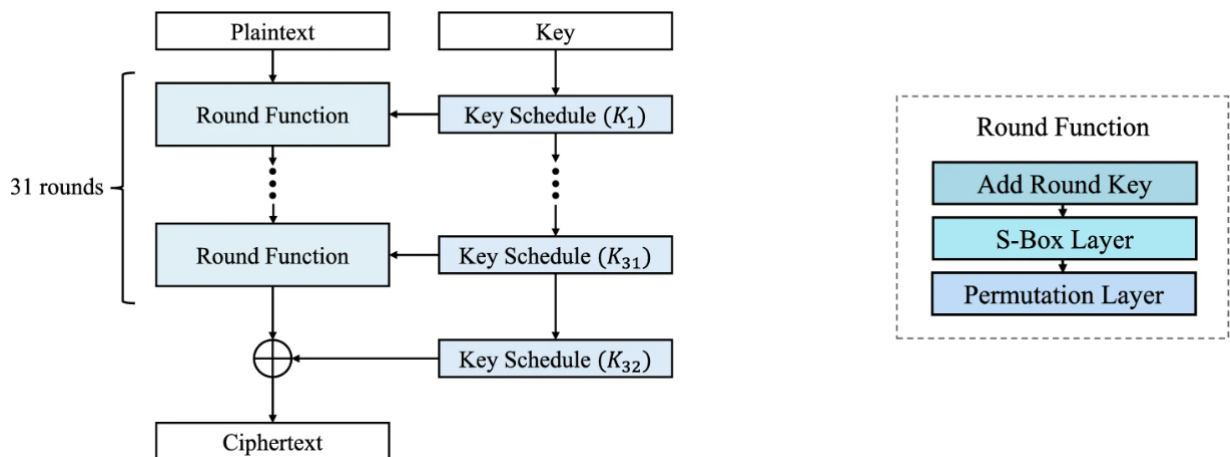


Рисунок 2.1 – Будова PRESENT [11]

Як вже зазначалося раніше шифр PRESENT є досить привабливим для використання в системах БпЛА серед інших блокових шифрів. Зокрема робота [9] оглядає декілька блокових, потокових шифрів та алгоритмів з перестановкою, щоб могли бути не поганими кандидатами для використання. Проте автори після їх аналізу все-таки виокремлюють та пропонують шістнадцятираундову модифікацію малоресурсного блокового шифру PRESENT в режимі лічильника.

Крім того, роботою чітко окреслюються вимоги до малоресурсних алгоритмів, які могли б використовуватися для шифрування відеопотоку дронів з обмеженими технічними характеристиками, особливо для БпЛА виду FPV. Це саме:

- час обробки відеопотоку (його шифрування та дешифрування) не має суттєво впливати на керування, тобто затримка не має перевищувати

0,03 секунди;

- пам'ять для зберігання кадру відеоданих не повинна при можливості перевищувати десятки мегабіт;

- алгоритм має забезпечити таке перетворення зображення, що внеможливише візуальне відтворення відкритого варіанту за шифротекстом;

- алгоритм повинен не допускати розповсюдження помилки, що при додаткових спотвореннях, перешкодить розшифруванню даних.

Зменшення раундів L16-PRESENT було проведено з 31 до 16, розмір блоку складає 64 біти, ключа — 80 біт, а режим лічильника обраний через найменше розповсюдження помилки серед розглянутих режимів. Результати аналізу наступні. Для атаки, що використовує диференціальний криптоаналіз, потрібно 2^{64} пар різних відкритих текстів, що навіть більше ніж всі можливі тексти — 2^{64} . Стверджується, що проведення такої атаки потребує 2^{32} МВ пам'яті, 2^{64} операцій та 2 місяці часу для зловмисника з більшими за стандартні обчислювальні можливості.

Запропонований на конференції «CYBERWARFARE: INTELLIGENCE, DEFENSE AND OFFENSIVE SECURITY» [10], восьмираундовий SP-шифр DONATION використовує 64 бітовий блок, 8-бітові S-блоки, 64-бітовий ключ. Саме модифіковані S-блок та перестановка збільшують швидкість шифрування в порівнянні з попереднім розглянутим алгоритмом. Збільшена також пропускна здатність, а потрібна пам'ять менша за 0.5KB.

Висновки до розділу 2

У підсумку, обидва алгоритми є досить ефективними, через свою структуру, та можуть бути використані для шифрування відеопотоку для пристроїв з обмеженими ресурсами. Стійкість у відповідних моделях теж достатня. Проте їх використання не в режимі лічильника, при умові

неідеального каналу, може призводити до сильного розповсюдження помилки.

3 МАЛОРЕСУРСНИЙ АЛГОРИТМ З ВЛАСТИВІСТЮ НЕРОЗПОВСЮДЖЕННЯ ПОМИЛКИ

Третій розділ містить опис запропонованого малоресурсного алгоритму для шифрування зображень, покращення для його реалізації, потрібний обсяг пам'яті, час роботи, стійкість до атаки перебору й недоліки в обраній моделі.

Враховуючи особливості алгоритмів, що були розглянуті в попередньому розділі, необхідні властивості, для наведеного нижче, визначаємо наступним чином: властивість нерозповсюдження помилки, за якою алгоритм не збільшує кількість неправильних байтів при пошкодженні даних в каналі; тимчасова стійкість, що складає від двох годин до кількох днів, залежно від поставлених перед пристроєм задач та можливостей злоумисника; кількість пам'яті для виконання, не враховуючи збереження зображення, не повинна перевищувати 10^6 бітів; швидкість шифрування та розшифрування при цьому не перевищує 0,3 секунди.

Позначмо $V_l = \{0,1\}^l$, $[n] = \{0,1,\dots,n-1\}$ для $n \in \mathbb{N}$ та будемо вважати, що екран з зображенням, за допомогою якого пілот взаємодіє з БПЛА, є прямокутним — $m < n$. Тоді один кадр відеопотоку можемо подати як прямокутну матрицю розмірності $[m] \times [n]$:

$$\Pi = (\pi_{ij})_{i,j=1}^{m,n},$$

де кожний елемент, залежно від того чи зображення кольорове, чи сіре, або $\pi \in V_{24}$, або $\pi \in V_8$, і є заповненням пікселів.

Тоді задача побудови алгоритму шифрування для введених позначень формалізується як побудова сімейства бієктивних відображень $\varphi : [m] \times [n] \rightarrow [m] \times [n]$, що є перестановкою пікселів на множині їх номерів з властивостями:

1) $\forall i \in [m] \exists 1 \leq j_1 < j_2 \leq n : \varphi(i, j_1) = (a_1, b_1)$ та $\varphi(i, j_2) = (a_2, b_2)$, де $a_1 \neq a_2$, тобто елементи матриці, які знаходилися в одному рядку, не обов'язково потраплять в один і той самий рядок;

2) $\forall j \in [n] \exists 1 \leq i_1 < i_2 \leq m : \varphi(i_1, j) = (a_1, b_1)$ та $\varphi(i_2, j) = (a_2, b_2)$, де $b_1 \neq b_2$, елементи, які знаходилися в одному стовпчику, теж не обов'язково потраплять в один і той самий стовпчик;

3) швидкість обчислення має бути невеликою, допустимою до вимог а використання пам'яті незначним.

Кожне таке перетворення з сімейства задаватиметься набором параметрів, множина яких і є ключовою для алгоритму. Правила шифрування та розшифрування в такому випадку:

$$C = E(\Pi), \text{ де } C = (\pi_{\varphi(i,j)})_{i,j=1}^{m,n}$$

$$\Pi = D(C), \text{ де } \Pi = (\pi_{\varphi^{-1}(i,j)})_{i,j=1}^{m,n}$$

. Тут φ^{-1} існує, бо φ — бієкція за умовою.

Далі розглядатимемо алгоритм, що використовує відображення $\varphi(i,j) = ((i + pj + r) \bmod m, (j + qi + s) \bmod n)$ з параметрами $p, r \in [m], q, s \in [n]$. В такому випадку, якщо вважати всі параметри допустимими для виконання бієктивності, потужність ключової множини $|K| = (mn)^2$. При, наприклад $m = 360, n = 420$ це $|K| = (360 \times 420)^2 = 22861440000 \approx 2^{34} \times 1.33071$, що може бути недостатнім навіть для тимчасової стійкості, в залежності від можливостей зловмисника та поставлених завдань для пристрою. Тому пропонується використовувати декілька раундів перетворення з різними ключами.

Як вже згадувалося вище, не всі набори ключів задовольняють умові бієктивності відображення φ і можуть бути використані для шифрування.

Твердження 3.1. *Відображення φ є бієктивним тоді і тільки*

тоді, коли система конгруенцій

$$\begin{cases} x + py \equiv 0 \pmod{m} \\ y + qx \equiv 0 \pmod{n} \end{cases}$$

має єдиний розв'язок на інтервалах

$$-(m-1) \leq x \leq m-1$$

$$-(n-1) \leq y \leq n-1$$

Доведення. Зазначимо, що множини визначень і значень відображення φ є скінченними і рівнопотужними. Тому бієктивність цього відображення буде еквівалентна його ін'єктивності.

Припустимо, що для двох різних пар (x_1, y_1) та (x_2, y_2) виконується рівність $\varphi_{p,r,q,s}(x_1, y_1) = \varphi_{p,r,q,s}(x_2, y_2)$. Що означає виконується система рівностей:

$$\begin{cases} (x_1 + py_1 + r) \pmod{m} = (x_2 + py_2 + r) \pmod{m} \\ (y_1 + qx_1 + s) \pmod{n} = (y_2 + qx_2 + s) \pmod{n} \end{cases}$$

що еквівалентно виконанню

$$\begin{cases} (x_1 + py_1) \pmod{m} = (x_2 + py_2) \pmod{m} \\ (y_1 + qx_1) \pmod{n} = (y_2 + qx_2) \pmod{n} \end{cases}$$

Позначимо $x = x_1 - x_2$ та $y = y_1 - y_2$, тоді остання система еквівалентна системі

$$\begin{cases} (x + py) \pmod{m} = 0 \\ (y + qx) \pmod{n} = 0 \end{cases}$$

Й умова того, що $(x_1, y_1) \neq (x_2, y_2)$ еквівалента умові, що система

$$\begin{cases} (x + py) \mod m = 0 \\ (y + qx) \mod n = 0 \end{cases}$$

має ненульовий розв'язок на інтервалах

$$-(m - 1) \leq x \leq m - 1$$

$$-(n - 1) \leq y \leq n - 1$$

□

Тобто при генерації набору ключів для шифрування потрібно перевіряти виконання умови твердження 3.1, що зменшує загальну кількість можливих ключів. А саме, розглядаючи $m = 360$ та $n = 420$, потужність ключової множини звужиться з приблизно 2^{34} до 2^{32} , що не є дуже суттєвим.

Також варто зауважити, що бієктивність не забезпечує зручного аналітичного обчислення оберненого відображення для розшифрування. Але розшифрування може бути здійснене й без обрахунку оберненого, з умовою тимчасового збереження матриці кадру. Тобто шифрування відбувається за правилом: елемент шифротексту для позиції (i, j) обчислюється $c_{i,j} = \pi_{\varphi(i,j)}$ зберігається; при розшифруванні та знаходженні позиції (i, j) для відкритого тексту Π обчислюється знову $\pi_{i,j} = c_{\varphi(i,j)}$. З чого складність розшифрування та шифрування однакова і складає $O(nt)$.

Оскільки відображення φ містить операцію приведення за модулем, що є досить ресурсноємною, його використання в початковому вигляді є неможливим для пристроїв з обмеженими ресурсами. Розглянемо додавання пам'яті, для збереження проміжних результатів обчислення, з метою підвищення швидкості алгоритму.

Нехай відображення $\varphi(i, j) = ((i + pj + r) \mod m, (j + qi + s) \mod n)$ це перетворення з фіксованими ключовими параметрами

$p, r \in [m]$, $q, s \in [n]$, побудуємо дворядкові таблиці T_p та T_q , що залежать від параметрів p та q відповідно. T_p складатиметься з усіх значень, що приймає j від 0 до $n - 1$, та величин $t_p(j) = (p \cdot j) \bmod m$, а таблиця T_q — з значень i від 0 до $m - 1$ та $t_q(i) = (q \cdot i) \bmod n$. Тоді, використовуючи таблиці, відображення можна переписати як

$$\varphi(i, j) = ((i + t_p(j) + r) \bmod m, (j + t_q(i) + s) \bmod n)$$

та повністю позбавитися виконання ділення за модулем у правій частині

$$(i + t_p(j) + r) \bmod m = \begin{cases} (i + t_p(j) + r), & \text{якщо } (i + t_p(j) + r) < m; \\ (i + t_p(j) + r - m), & \text{якщо } m \leq (i + t_p(j) + r) < 2m; \\ (i + t_p(j) + r - 2m), & \text{якщо } (i + t_p(j) + r) \geq 2m. \end{cases}$$

$$(i + t_q(i) + s) \bmod n = \begin{cases} (i + t_q(i) + s), & \text{якщо } (i + t_q(i) + s) < n; \\ (i + t_q(i) + s - n), & \text{якщо } n \leq (i + t_q(i) + s) < 2n; \\ (i + t_q(i) + s - 2n), & \text{якщо } (i + t_q(i) + s) \geq 2n. \end{cases}$$

Такі обчислення будуть коректними, бо значення $i, t_p(i), r$ згідно визначення лежать в межах від 0 до $m - 1$ та їх сума не перевищує $3m$, що виконується аналогічно і для іншої частини n .

Для оцінки пам'яті знову розглянемо кадр розміру 360×420 , де $mn = 151200$ пікселів. При збереженні такого зображення у сірому форматі де піксель займає 1 байт потрібно 151200 байтів або 1209600 бітів. При ж кольоровому RGB вигляді та трьома байтами на піксель потрібно 453600 байтів або 3628800 бітів. Лише розмір зображення впливає на пам'ять для його збереження, а не параметри алгоритму. Щодо ключів $p, r \in [m]$, $q, s \in [n]$, в нашому випадку, кожен з параметрів можна подати 9 бітами, оскільки $2^8 < 420 < 2^9$. Звідси мінімальний обсяг пам'яті для зберігання це 36 бітів, що на практиці може бути виконано як збереження чотирьох беззнакових 16-бітних змінних. Разом це — 64 біти

або 8 байтів для всього ключа. При збереженні двох таблиць достатньо зберігати лише значення $t_p(j)$ та $t_q(i)$, де кожне не перевищує $n = 420$, тобто 9 бітів. Отже потрібна пам'ять це $(m + n) \cdot 9 = 780 \cdot 9 = 7020$ бітів, чи приблизно 878 байтів. З використанням 16-бітових змінних на практиці $(m + n) \cdot 16 = 780 \cdot 16 = 12480$ або 1560 байтів.

Аналізуючи час роботи алгоритму, можемо сказати що побудова попередньо обчислених таблиць є важливою для малоресурсної реалізації. Адже, саме це замінює дві операції приведення за модулем на звернення до пам'яті алгоритму, кількома додаваннями, відніманнями та порівняннями. Для одного кадру операції шифрування потрібно пройти по $m \cdot n = 151200$ пікселях, як і ,вже зазначалося раніше, розшифруванню теж. Тобто загальна кількість позицій, що оброблюється, для одного кадру дорівнює $2 \cdot mn = 302400$. Щоб весь час обробки не перевищував 0.3 секунди, середній час на позицію не має бути більшим за $0.3/(2mn) \approx 9.9 \cdot 10^{-7}$ секунди, тобто приблизно 1 мс на піксель. Для сірого зображення це 1 Мпкс/с, а для RGB-зображення — 1.8 Мбайта за 0.3 секунди, що звичайно не враховує витрат на організацію пам'яті та керування. Тобто, за теоретичною оцінкою, обмеження в 0.3 секунди є реалістичним для типового чи сигнального процесора, при обчисленні таблиць для конкретного ключа заздалегідь. Але фактично час роботи ще залежить від архітектури процесора, кешу, швидкості доступу до пам'яті, способу зберігання кадру та формату пікселя, тому попередня наведена оцінка, безумовно, ще потребує експериментальної перевірки на цільових апаратних платформах.

Розглянемо також стійкість алгоритму до атаки перебору, для одного кадру та умови, що злоумисник знає структуру алгоритму, але не параметри p, r, q, s . Оцінка, для повного простору параметрів з потужністю $|K| = 2^{34.4}$ та злоумисником, що може перевіряти R ключів на секунду, виглядає як $T = |K|/R$. Наприклад при $R = 10^5$ ключів/с час повного перебору складатиме $T = 63.5$ години , при $R = 10^6$ ключів/с — приблизно 6.35 години, а при $R = 10^7$ ключів/с — приблизно 38 хвилин.

Межа зламу у дві години відповідатиме приблизно $3.2 \cdot 10^6$ ключів/с. Отже, одна ітерація відображення забезпечуватиме стійкість тільки проти зловмисника з помірними технічними можливостями та відсутністю кращого способу перевірки правильності ключа. Для збільшення часу стійкості до декількох діб або в моделі з сильнішим зловмисником рекомендується використовувати декілька незалежних ітерацій та обмежувати час використання ключа. Крім того, варто зауважити, що на перетворення такого виду, існують швидші за перебір атаки. Тому оцінка вище не є оцінкою повної криптографічної стійкості алгоритму.

Серед подібних атак, до яких алгоритм може бути слабким, є атаки з відомим відкритим текстом. Оскільки запропоноване перетворення є лише перестановкою місць пікселів, а не зміною їх значень, шифротекст зберігає кольори та гістограму яскравості зображення. Для кадрів з горизонтом, великими однорідними областями, такими як небо, дорога, статистичні ознаки можуть зберігатися, що дає зловмиснику перевагу у розпізнаванні та відновленні структури зображення. Відомо [12], що шифри для медіа, які використовують лише перестановки, можуть бути зламані з використанням $O([\log_L(MN)])$ відкритих текстів, де L — кількість різних елементів тексту, а $M \times N$ — розмірність зображення. Крім того, в деяких випадках атаки можуть бути побудовані навіть на ті алгоритми, що використовують не лише перестановки [13]. Тобто, якщо зловмисник має доступ до пари відкритого і шифрованого тексту для одного й того ж ключа, він отримує інформацію про перестановку позицій пікселів. Через що, в моделі тимчасової стійкості, краще припускати, що зловмисник не має можливості провести атаку з вибраними відкритими текстами.

Крім того, додатковим джерелом інформації з відеопотоку для зловмисника є кадри, що майже не змінюються, тобто сцени, які рухаються повільно. Якщо ключ використовується занадто довго, можливе накопичення статистичних даних. Тому час дії ключових параметрів має бути обмеженим для невеликої кількості кадрів.

Також запропоноване відображення залежить від чотирьох параметрів та має лінійний вигляд за координатами пікселів, що робить його вразливим за структурою. При вдалому відновленню достатньої кількості позицій відкритого та шифрованого тексту, зломисник може відновити систему модульних співвідношень для ключових параметрів. Тобто, як вже зазначалося раніше, стійкість алгоритму не може бути визначена лише стійкістю до перебору ключів. Через, що залишається необхідність в обмеженні моделі зломисника й експериментальній перевірці впізнаваності певних видів зображення після шифрування.

Але навіть з урахуванням згаданих обмежень алгоритм може бути застосованим в практичних сценаріях. Наприклад у випадках постійного руху БпЛА, де кадри часто змінюється через кут нахилу, освітлення, положення камери, масштаб об'єктів. Зміна ключа для фіксованої кількості кадрів чи в визначений проміжок часу теж збільшить допустимість такої моделі.

Висновки до розділу 3

Наведені в розділі оцінки пам'яті та часу роботи є попередніми, ґрунтуються на підрахунку елементарних операцій й потрібної службової пам'яті, не враховують всіх особливостей БпЛА, таких як частоту процесора, пропускну здатність пам'яті, подання кадру, спосіб доступу до відеобуферу, енергоспоживання і тому подібне. Крім того саме перетворення не забезпечує цілісність та автентичність даних. Захист від активного зломисника має бути забезпечений іншими способами.

У підсумку, запропонований алгоритм слід розглядати як малоресурсний тимчасовий спосіб захисту відеопотоку тільки для моделі з коротким часом використання ключа, форматом подання кадру, що є сумісним з властивістю нерозповсюдження помилки, та обмеженими обчислювальними можливостями зломисника, в тому числі й відсутністю доступу до вибраних відкритих зображень.

Остаточна оцінка алгоритму також має включати не тільки теоретичні підрахунки, а й експериментальні вимірювання часу роботи, пам'яті, енергоспоживання та візуальної якості маскування відеопотоку. Для остаточного висновку про придатність алгоритму до практичного використання потрібні експерименти на платформах максимально близьких до згаданих.

ВИСНОВКИ

У ході роботи було проведено огляд наукових джерел за темою малоресурсних алгоритмів для шифрування відеопотоку з властивістю нерозповсюдження помилки. В результаті чого було визначено, що для БпЛА багато рішень є або занадто ресурсоємними, або тими що не є достатніми в умовах неідеального каналу. Використання перестановок показує найкращі результати для поставлених вимог.

Огляд шифрів L16-PRESENT та DONATION показує, що вони мають достатню тимчасову стійкість та малоресурсність для шифрування відеопотоків БпЛА, але не є рішеннями для проблеми розповсюдження помилки при неідеальному каналі зв'язку.

Аналіз алгоритму у роботі складав: оцінку пам'яті, часу роботи; покращення потрібні для реалізації; обговорення обмежень моделі, можливих статистичних атак, атак на структуру й атак з відкритими текстами; визначення стійкості до атаки перебору. З чого було зроблено висновок, що запропонований алгоритм для наведених попередніх оцінок потребує ще практичного експериментального дослідження на апаратних платформах максимально близьких до БпЛА.

Як підсумок можна сказати найкращим використанням алгоритму є тимчасове малоресурсне маскування відеопотоку в випадках, коли зломисник має лише пасивний доступ до каналу й не має можливості отримувати пари відкритих та шифрованих текстів одного ключа, а корисність перехопленої інформації зменшується з часом.

ПЕРЕЛІК ПОСИЛАНЬ

- [1] Bryce Cordill, Dongfeng Fang та Shengjie Xu. «A Comprehensive Survey of Security and Privacy in UAV Systems». B: *IEEE Access* 13 (2025), с. 117843—117866. DOI: 10.1109/ACCESS.2025.3583985.
- [2] Sayani Sarkar та ін. «Secure Communication in Drone Networks: A Comprehensive Survey of Lightweight Encryption and Key Management Techniques». B: *Drones* 9.8 (2025). ISSN: 2504-446X. DOI: 10.3390/drones9080583. URL: <https://www.mdpi.com/2504-446X/9/8/583>.
- [3] Samina Jadoon та ін. «A survey of image encryption schemes: Arnold transformation, chaos, bit-plane extraction and permutation based algorithms». B: *Multimedia Tools and Applications* 85.3 (2026), с. 210.
- [4] Hegui Zhu та ін. «An image encryption scheme using generalized Arnold map and affine cipher». B: *Optik* 125.22 (2014), с. 6672—6677.
- [5] Mehmet Turan, Erhan Gökçay та Hakan Tora. «An unrestricted Arnold's cat map transformation». B: *Multimedia Tools and Applications* 83.28 (2024), с. 70921—70935.
- [6] Jie Dong та ін. «The improved image scrambling algorithm for the wireless image transmission systems of UAVs». B: *Sensors* 18.10 (2018), с. 3430.
- [7] Orkhan Valikhanli та Fargana Abdullayeva. «Securing UAV Flight Data Using Lightweight Cryptography and Image Steganography.» B: *International Journal of Advanced Computer Science & Applications* 16.5 (2025).
- [8] Dong Jiang та ін. «Real-Time Bit-Level Encryption of Full High-Definition Video Without Diffusion». B: *arXiv preprint arXiv:2505.07158* (2025).

- [9] Liudmyla Kovalchuk та ін. «Development of an algorithm with temporary cryptographic security for encrypting video stream from an unmanned aerial vehicle». B: *Eastern-European Journal of Enterprise Technologies* 5.9 (137) (2025), 41–53. DOI: 10.15587/1729-4061.2025.340917. URL: <https://journals.uran.ua/eejet/article/view/340917>.
- [10] L.V. Kovalchuk та ін. «DONATION: A Lightweight Block Cipher for UAV Application». B: 2026. URL: <https://cyberwarfare.viti.edu.ua/>.
- [11] Valérie Gauthier-Umaña та ін. «Key recovery attack on PRESENT using an entropy-based neural distinguisher». B: *Neural Computing and Applications* 38.9 (2026), с. 305.
- [12] Chengqing Li та Kwok Tung Lo. «Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks». B: *Signal Processing* 91.4 (2011), с. 949–954.
- [13] Ming Li та ін. «Cryptanalysis of permutation–diffusion-based lightweight chaotic image encryption scheme using CPA». B: *Applied Sciences* 9.3 (2019), с. 494.