

МЕТОДИ ВИЯВЛЕННЯ ТА ВИЛУЧЕННЯ ПРИХОВАНОЇ ІНФОРМАЦІЇ, ВБУДОВАНОЇ У ЗОБРАЖЕННЯ З ВИКОРИСТАННЯМ СТЕГАНОГРАФІЇ

ВИКОНАЛА СТУДЕНТКА БІКС-23С: СЕРГІЄНКО БОГДАНА
КЕРІВНИК РОБОТИ: ШАБАЛА ЄВГЕНІЯ ЄВГЕНІВНА

АКТУАЛЬНІСТЬ РОБОТИ



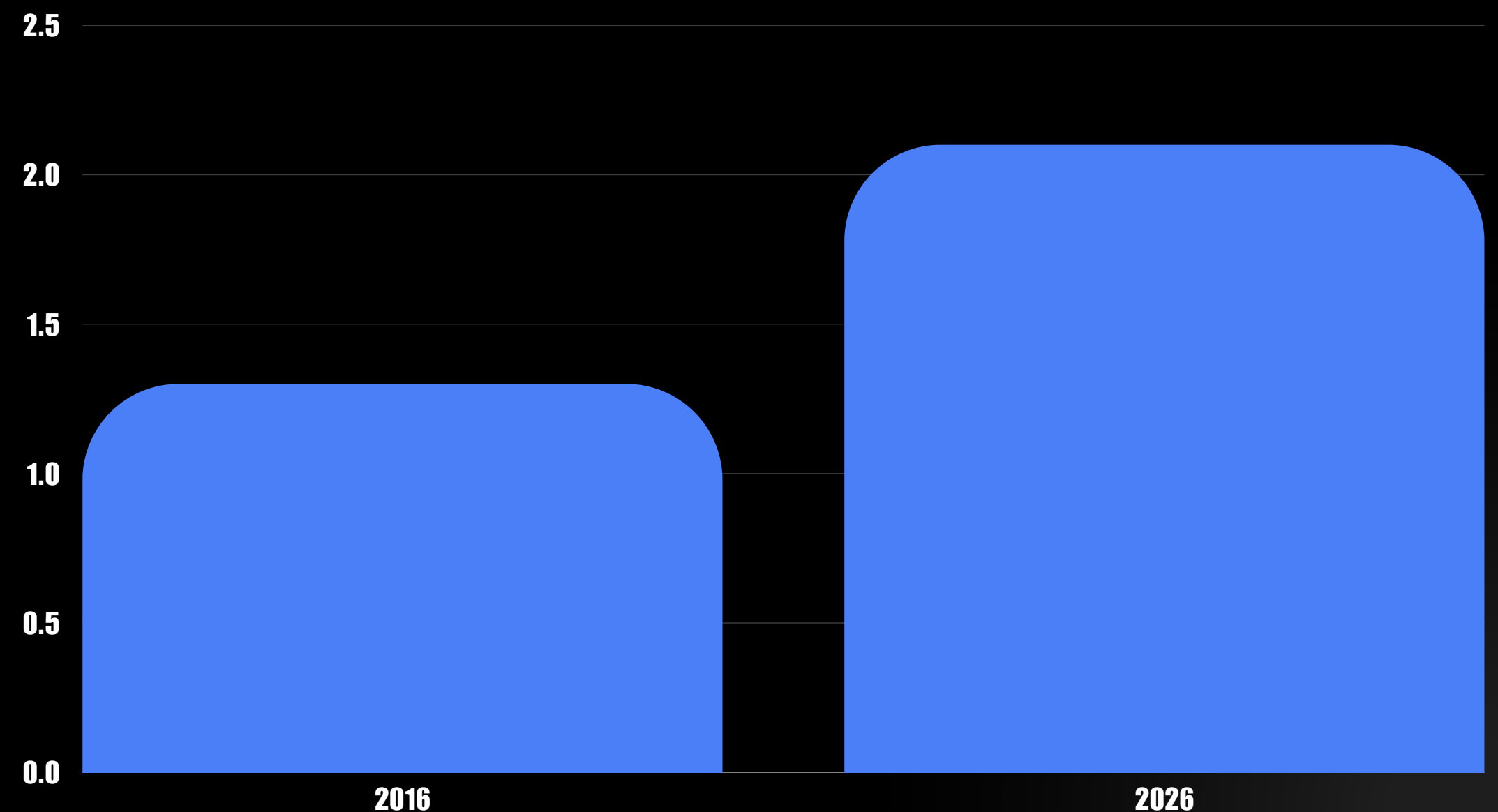
Зростання обсягів цифрового та синтетичного контенту підвищує ризик використання зображень як контейнерів прихованої передачі даних.

2.1 ТРЛН ФОТО/РІК

**15+ МЛРД AI-
ЗОБРАЖЕНЬ З 2022
РОКУ**

57 ТИС. ФОТО/С

Світовий обсяг фото на рік (трлн)



МЕТА, ОБ'ЄКТ, ПРЕДМЕТ ТА ЗАВДАННЯ ДОСЛІДЖЕННЯ

Мета роботи

РОЗРОБИТИ МЕТОД ВІЯВЛЕННЯ ТА ВИЛУЧЕННЯ ПРИХОВАНОЇ ІНФОРМАЦІЇ У ЦИФРОВИХ ЗОБРАЖЕННЯХ З УРАХУВАННЯМ ОСОБЛИВОСТЕЙ СИНТЕТИЧНИХ **3D**-РЕНДЕРІВ.

Об'єкт
дослідження

ПРОЦЕСИ ПРИХОВАНОГО ВБУДОВУВАННЯ ТА ВІЯВЛЕННЯ ІНФОРМАЦІЇ У ЦИФРОВИХ ЗОБРАЖЕННЯХ.

Предмет
дослідження

МЕТОДИ СТЕГОАНАЛІЗУ **LSB**-ВБУДОВУВАННЯ У ПРИРОДНИХ І СИНТЕТИЧНИХ ЗОБРАЖЕННЯХ.

Завдання
дослідження

- ✓ проаналізувати сучасні методи стеганографії та стегоаналізу.
- ✓ дослідити особливості синтетичних зображень як стеганографічних контейнерів.
- ✓ розробити комбінований метод виявлення.
- ✓ реалізувати програмний засіб.
- ✓ провести базову експериментальну перевірку.

ОСОБЛИВОСТІ 3D-РЕНДЕРІВ ЯК КОНТЕЙНЕРІВ

Чому 3D-рендери цікаві як стеганографічні контейнери

Критерій	Фотографія	3D-рендер
Походження шуму	природний	контрольований / штучний
Структура зображення	залежить від камери	залежить від сцени та рендерингу
Повторюваність	нижча	вища
Передбачуваність	нижча	вища
Потенціал для маскування	середній	може бути вищим

ФОТОГРАФІЯ



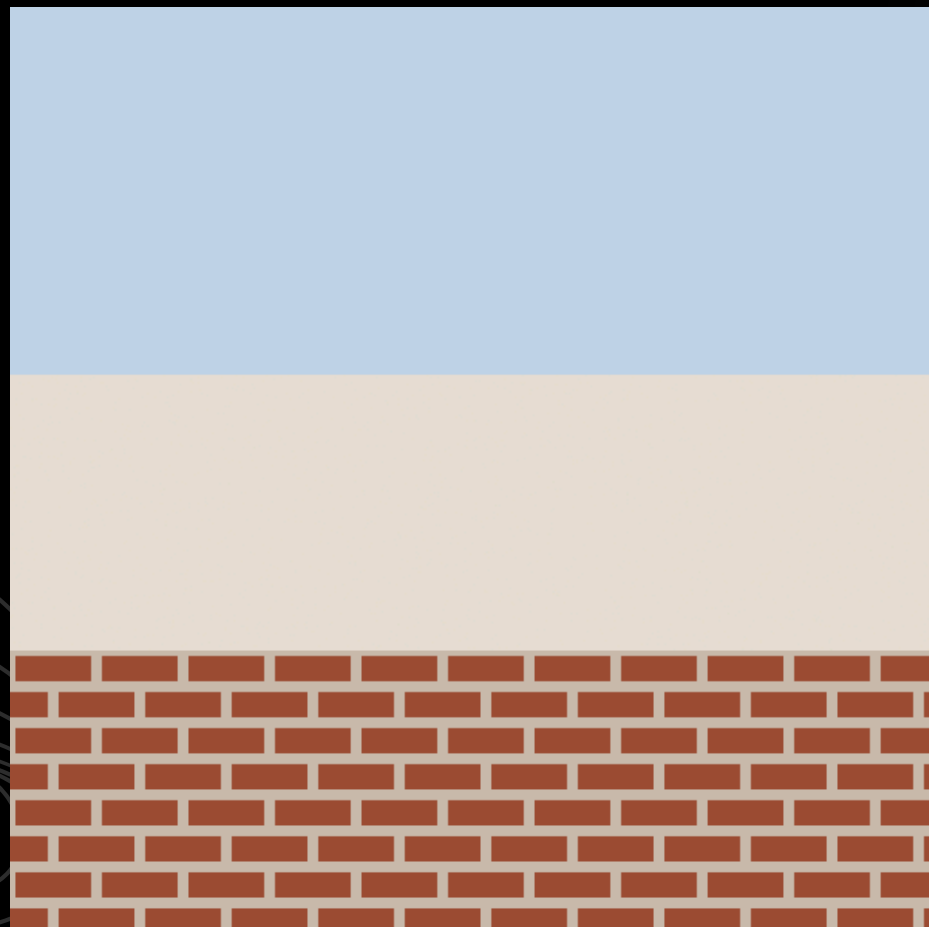
3D-РЕНДЕР



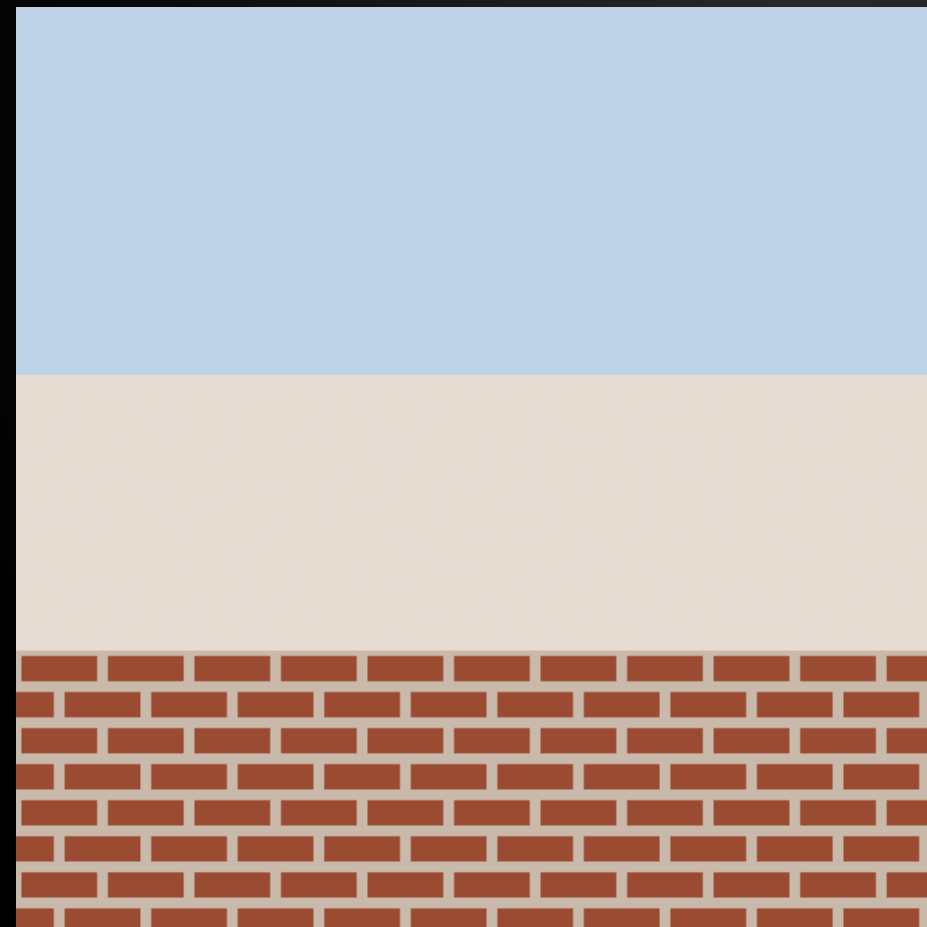
БІТОВІ ПЛОЩИНИ ТА ОЗНАКИ ВБУДОВУВАННЯ

Візуально стегозображення часто майже не відрізняється від оригіналу. Основні зміни проявляються на рівні молодших бітів.

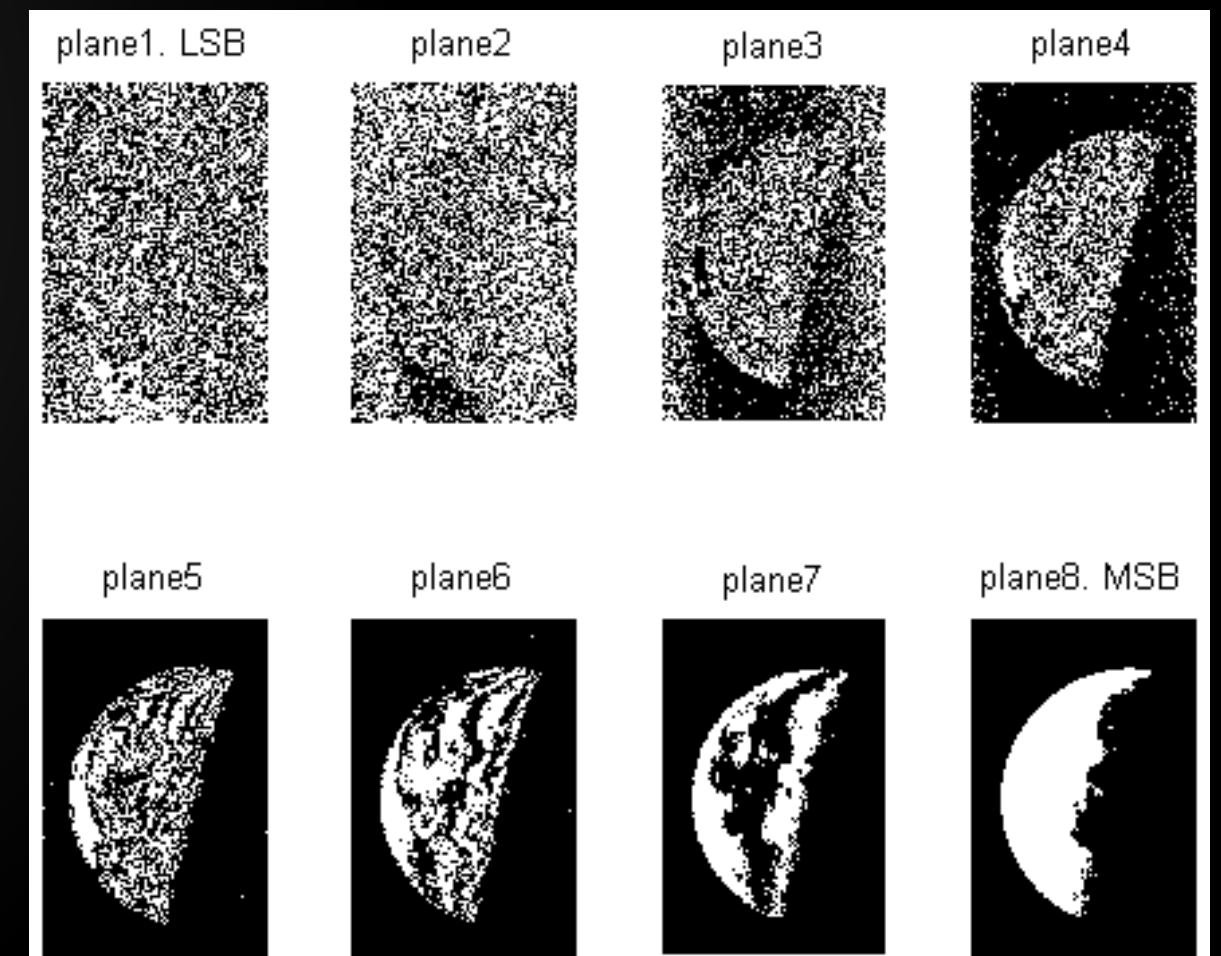
Саме тому аналіз бітових площин є базовим етапом запропонованого методу.



ЗОБРАЖЕННЯ ДО
ВБУДОВУВАННЯ ДАНИХ



ЗОБРАЖЕННЯ ПІСЛЯ
ВБУДОВУВАННЯ ДАНИХ



БІТОВІ ПЛОЩИНИ

МЕТОДИКА ДОСЛІДЖЕННЯ

Крок 1 — Знайти "шум" там, де його не повинно бути

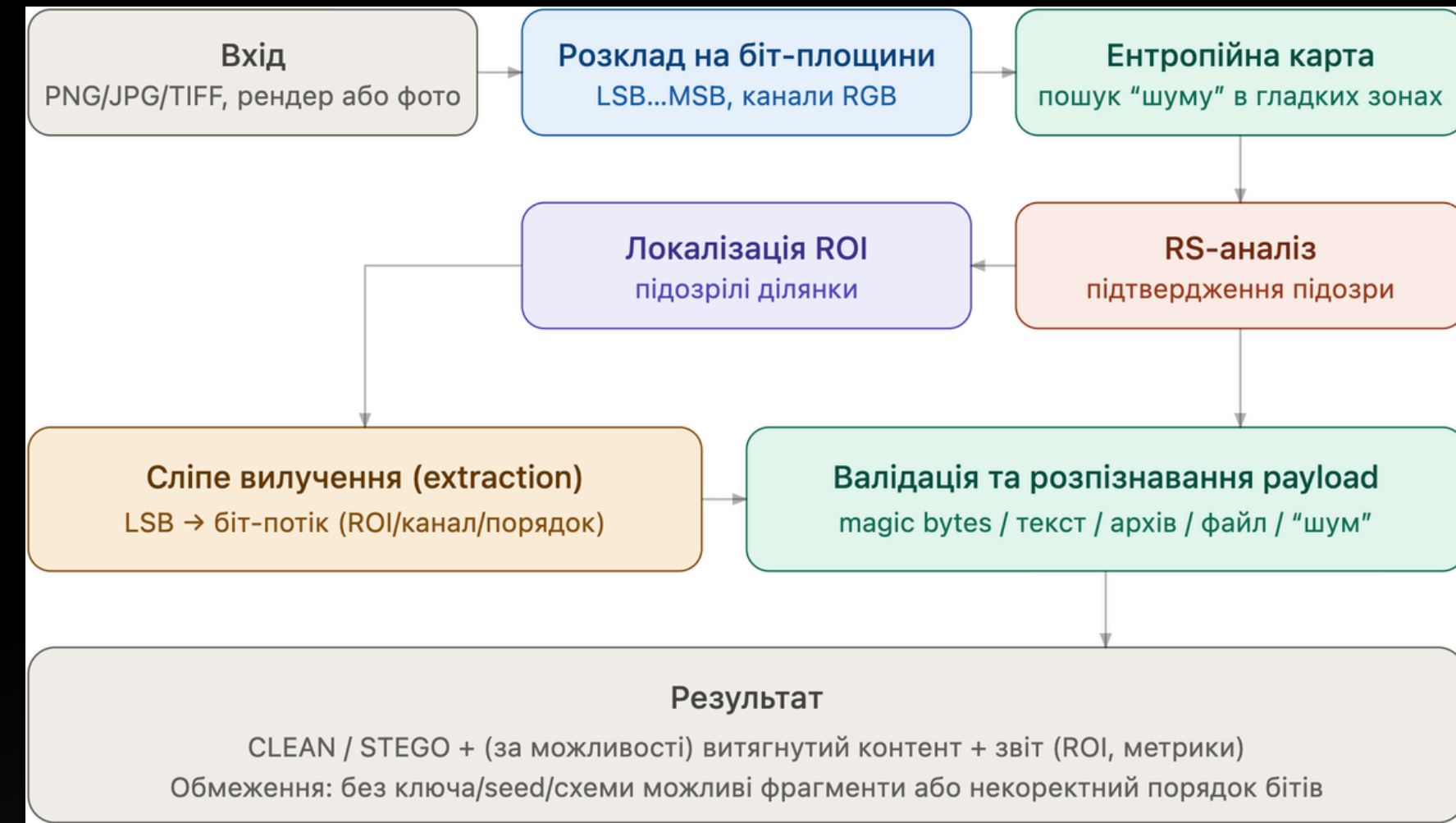
Найменший біт кожного пікселя (LSB) у чистому рендері поводить себе передбачувано — гладкі стіни, рівні поверхні дають майже нульовий "хаос". Якщо хтось сховав там дані — хаос різко зростає.

Крок 2 — Підтвердити підозру математично

Там, де ентропія підозріло висока, запускаємо RS-аналіз — метод, розроблений дослідницею Джессікою Фрідріх

Крок 3 — Витягнути і розпізнати

Якщо факт вкладення підтверджено — програма витягує ці біти і намагається зрозуміти що це: текст, зашифрований файл, архів або зображення.



ВИЛУЧЕННЯ ПРИХОВАНОЇ ІНФОРМАЦІЇ

1. Формування бітового потоку

- Вилучення LSB-бітів
- Побудова послідовності байтів



2. Аналіз payload

- Текст
- Зображення
- Архів
- Шифровані дані



3. Результат

- Відновлені дані
- Звіт про вилучення

ЗОБРАЖЕННЯ 



LSB-БІТИ Least Significant Bit 1011100**1**



БІТОВИЙ ПОТІК



ТИП ДАНИХ



ТЕКСТ / АРХІВ /
ЗОБРАЖЕННЯ

ПРОГРАМНА РЕАЛІЗАЦІЯ

Steganography Detector

Multi-stage LSB steganography analysis for 3D renders (3ds Max / V-Ray / Corona).

Upload Image (PNG / JPG / TIFF)

Window Size

Block size for entropy computation (8 / 16 / 32 / 64)

8 16 64

Entropy Threshold

Base threshold for suspicious block detection

0.3 0.7 1

☐ Attempt Blind Extraction

Chi-Square Analysis Region

☒ Auto-find smoothest region

Automatically selects the region with lowest LSB entropy — best for real renders

Or set manual region (% of image):

X %

0 90

Y %

0 90

W %

5 100

H %

5 100

ANALYZE

Overview Visual Analysis RS Analysis Extraction Chi-Square Report

× STEGO DETECTED

Entropy Min

0.0000

Entropy Max

1.0000

Entropy Mean

0.2216

Suspicious ROI zones found

128

Estimated payload (RS cumulative)

—

У межах роботи розроблено програмний засіб на Python для аналізу цифрових зображень, який забезпечує:

- виділення бітових площин;
- побудову ентропійної карти;
- локалізацію підозрілих ділянок;
- локальний RS-аналіз;
- спробу сліпого вилучення даних.

Steganography Detector

Multi-stage LSB steganography analysis for 3D renders (3ds Max / V-Ray / Corona).

Upload Image (PNG / JPG / TIFF)

Overview

Visual Analysis

RS Analysis

Extraction

Chi-Square

Report

X STEGO DETECTED

Entropy Min

0.0000

Entropy Max

1.0000

Entropy Mean

0.2216

Suspicious ROI zones found

128

Estimated payload (RS cumulative)

—

Window Size

Block size for entropy computation (8 / 16 / 32 / 64)

8

64

Entropy Threshold

Base threshold for suspicious block detection

0.3

0.7

1

Attempt Blind Extraction

Chi-Square Analysis Region

Auto-find smoothest region

Automatically selects the region with lowest LSB entropy — best for real renders

Or set manual region (% of image):

X %

0

90

Y %

0

90

W %

100

5

H %

100

5

ANALYZE

Steganography Detector

Multi-stage LSB steganography analysis for 3D renders (3ds Max / V-Ray / Corona).

Upload Image (PNG / JPG / TIFF)

Overview

Visual Analysis

RS Analysis

Extraction

Chi-Square

Report

Original Image

Entropy Heatmap Overlay

Highlighted Anomaly Zones

USB Plane - R channel

USB Plane - G channel

USB Plane - B channel

ANALYZE

Steganography Detector

Multi-stage LSB steganography analysis for 3D renders (3ds Max / V-Ray / Corona).

Upload Image (PNG / JPG / TIFF)

Overview

Visual Analysis

RS Analysis

Extraction

Chi-Square

Report

RS-Analysis Results

Zone ID	X	Y	Width	Height	R groups	S groups	Probability %
1	0	0	16	16	0.3750	0.3125	100.0%
2	16	0	16	16	0.2188	0.2656	100.0%
3	32	0	16	16	0.3281	0.2969	100.0%
4	48	0	16	16	0.2031	0.2500	100.0%
5	64	0	16	16	0.2031	0.1562	100.0%
6	80	0	16	16	0.2500	0.2656	100.0%
7	96	0	16	16	0.2344	0.1719	100.0%
8	112	0	16	16	0.1719	0.2812	100.0%
9	128	0	16	16	0.3594	0.2969	100.0%
10	144	0	16	16	0.2812	0.2188	100.0%
11	160	0	16	16	0.2500	0.1719	100.0%
12	176	0	16	16	0.2500	0.2500	100.0%

Window Size

Block size for entropy computation (8 / 16 / 32 / 64)

8

64

Entropy Threshold

Base threshold for suspicious block detection

0.3

0.7

1

Attempt Blind Extraction

Chi-Square Analysis Region

Auto-find smoothest region

Automatically selects the region with lowest LSB entropy — best for real renders

Or set manual region (% of image):

X %

0

90

Y %

0

90

W %

100

5

H %

100

5

ANALYZE

Steganography Detector

Multi-stage LSB steganography analysis for 3D renders (3ds Max / V-Ray / Corona).

Upload Image (PNG / JPG / TIFF)

Overview

Visual Analysis

RS Analysis

Extraction

Chi-Square

Report

Enable Attempt Blind Extraction and run ANALYZE.

Payload Entropy (0–8 bits)

4.6034

Detected Type

binary

Magic Bytes Found

None

Extracted Text Preview (first 200 chars)

(binary / encrypted)

Download raw extracted .bin

tmpvztmujn.bin

4.0 KB

Window Size

Block size for entropy computation (8 / 16 / 32 / 64)

8

64

Entropy Threshold

Base threshold for suspicious block detection

0.3

0.7

1

Attempt Blind Extraction

Chi-Square Analysis Region

Auto-find smoothest region

Automatically selects the region with lowest LSB entropy — best for real renders

Or set manual region (% of image):

X %

0

90

Y %

0

90

W %

100

5

H %

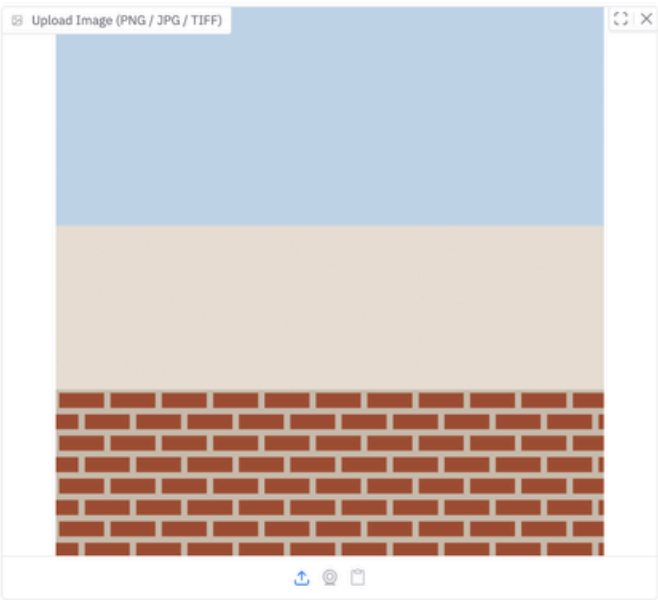
100

5

ANALYZE

Steganography Detector

Multi-stage LSB steganography analysis for 3D renders (3ds Max / V-Ray / Corona).



Window Size
Block size for entropy computation (8 / 16 / 32 / 64)

8 64

Entropy Threshold
Base threshold for suspicious block detection

0.3 1

☐ Attempt Blind Extraction

Chi-Square Analysis Region

☒ Auto-find smoothest region
Automatically selects the region with lowest LSB entropy — best for real renders

Or set manual region (% of image):

X % 0 90 Y % 0 90

W % 100 5 H % 100 5

ANALYZE

Overview Visual Analysis RS Analysis Extraction Chi-Square Report

✓ CLEAN

Entropy Min	Entropy Max	Entropy Mean
0.0000	0.3671	0.1382

Suspicious ROI zones found

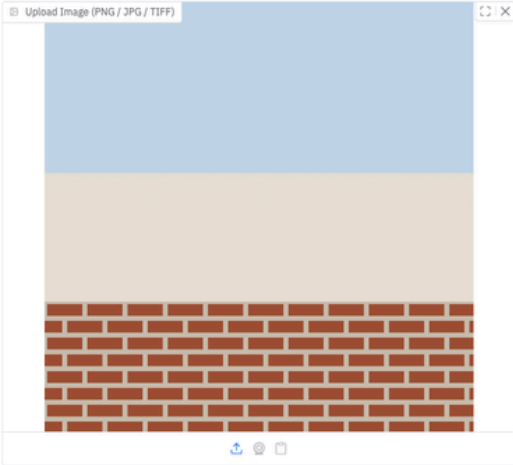
0

Estimated payload (RS cumulative)

—

Steganography Detector

Multi-stage LSB steganography analysis for 3D renders (3ds Max / V-Ray / Corona).



Window Size
Block size for entropy computation (8 / 16 / 32 / 64)

8 64

Entropy Threshold
Base threshold for suspicious block detection

0.3 1

☐ Attempt Blind Extraction

Chi-Square Analysis Region

☒ Auto-find smoothest region
Automatically selects the region with lowest LSB entropy — best for real renders

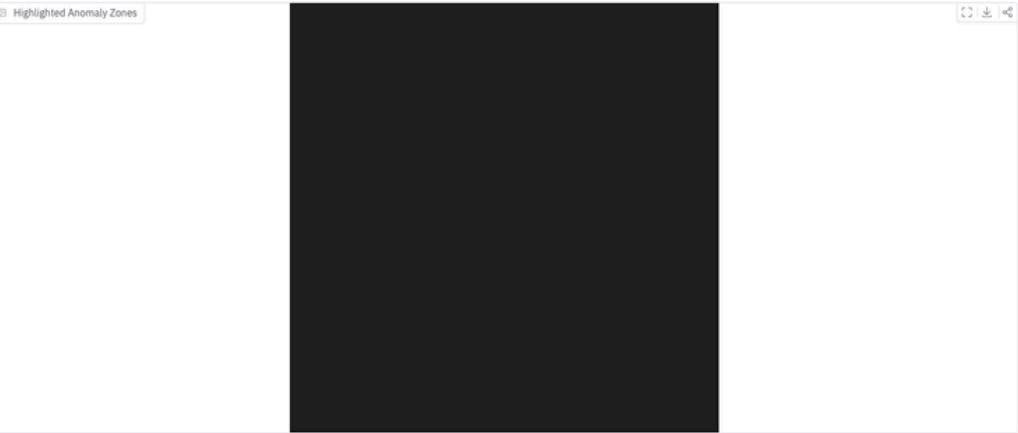
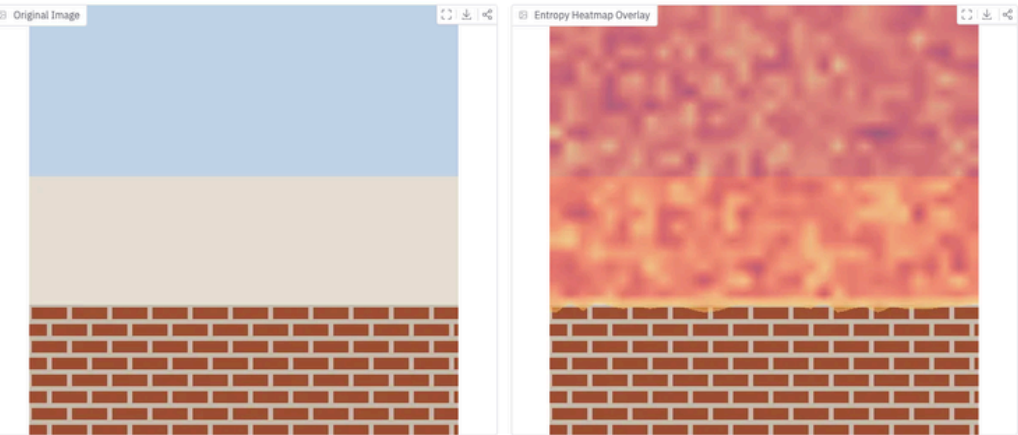
Or set manual region (% of image):

X % 0 90 Y % 0 90

W % 100 5 H % 100 5

ANALYZE

Overview Visual Analysis RS Analysis Extraction Chi-Square Report



ЕКСПЕРИМЕНТАЛЬНА БАЗА ДОСЛІДЖЕННЯ

Для перевірки методу було використано контрольовану вибірку синтетичних рендерів, сформовану зі сцен:

- з великими однорідними областями;
- невисокою локальною ентропією;
- чіткими контурами об'єктів;
- мінімальною кількістю дрібних текстурних деталей.



РЕЗУЛЬТАТИ БАЗОВОГО ТЕСТУВАННЯ НА КОНТРОЛЬОВАНИХ РЕНДЕРАХ

У межах базового тестування встановлено, що на спрощених синтетичних рендерах запропонований метод дозволяє:

- виявляти структурні аномалії в бітових площинах;
- локалізувати потенційно підозрілі ділянки за допомогою ентропійного аналізу;
- застосовувати локальний RS-аналіз до вибраних областей;
- виконувати базову перевірку наявності прихованого вбудовування в умовах низької локальної ентропії.

Тип сцени	Спостереження
Однорідні області	аномалії помітніші
Чіткі контури	локалізація простіша
Низька ентропія	метод працює стабільніше
Складні текстури	потрібен локальний аналіз

ОБМЕЖЕННЯ ДОСЛІДЖЕННЯ ТА ПЕРСПЕКТИВИ

Обмеження:

- тестування проводилося на контрольованій вибірці спрощених синтетичних рендерів;
- високодеталізовані фотореалістичні сцени мають вищу локальну ентропію;
- для складних рендерів потрібен фрагментний аналіз окремих ділянок.

Перспективи розвитку:

- автоматичний вибір підозрілих областей;
- адаптація методу до складних текстурованих сцен;
- розширення експериментальної вибірки;
- застосування до анімованих та відеоданих.



ВИСНОВКИ ТА ПРАКТИЧНЕ ЗНАЧЕННЯ

У результаті виконання роботи:

- проаналізовано стеганографічні загрози у цифрових зображеннях;
- досліджено особливості синтетичних 3D-рендерів як потенційних контейнерів;
- розроблено комбінований метод виявлення та вилучення прихованої інформації;
- реалізовано програмний засіб для аналізу зображень;
- виконано базову експериментальну перевірку методу на контрольованій вибірці синтетичних рендерів.

Практичне значення:

- первинний аналіз підозрілих зображень;
- навчальні та дослідницькі задачі у сфері кібербезпеки;
- цифрова криміналістика;
- подальший розвиток методів стегоаналізу для синтетичних медіаданих.

ДЯКУЮ