



# Порівняння ефективності класів стеганографічних алгоритмів

Грициндишина Віталія Любомировича

24 травня 2022 р.

## 1 Постановка задачі

- Актуальність теми
- Задача та класифікація стеганографії
- Математична постановка задачі

## 2 Структури мультимедійних даних

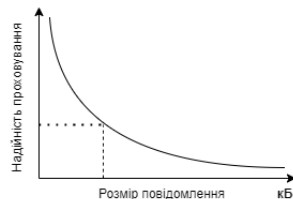
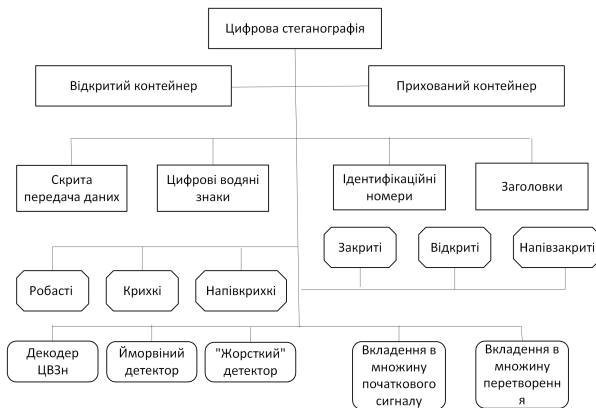
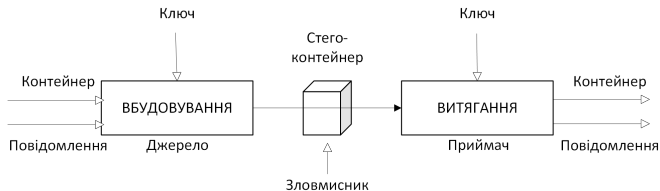
- Приховування інформації у нерухомих зображеннях
- Приховування інформації у текстових файлах
- Приховування інформації в аудіосигналах
- Оцінка ефективності стеганоситеми

## 3 Приклади застосування

- Приховування даних в BMP форматі методом заміни найменш значущого біта

## 4 Висновки





$$E : C \times M \rightarrow S; \quad (1)$$

$$D : S \rightarrow M, \quad (2)$$

$$\sum (C, M, S, E, D) \quad (3)$$

$$\text{sim}[c, E(c, m)] = 1, \forall m \in M, c \in C \quad (4)$$

$$c = \max(\text{sim}[x, E(x, m)]) \quad (5)$$

$$E(c, m) \approx E(c + \delta, m) \quad D[E(c, m)] \approx D[E(c + \delta, m)] = m \quad (6)$$

де  $S = \{(c_1, m_1), (c_2, m_2), \dots, (c_q, m_q), \} = \{s_1, s_2, \dots, s_q\}$  - множина стеганограм (заповнених контейнерів),  $m_a, m_b \in M$ ,  
 $(c_a, m_a), (c_b, m_b) \in S$

Деякі методи приховування даних:

- Метод заміни найменш значущого біта;

(00100111	11101001	11001000)
(00100111	11001000	11101001)
(11001000	00100111	11101001)

↓ 10000001 ↓

(00100111	1110100 <u>0</u>	11001000)
(0010011 <u>0</u>	11001000	1110100 <u>0</u> )
(11001000	00100111	11101001)

- Метод маскування та фільтрації;

- Метод перетворення;

$$F(u, v) = \frac{1}{4}C(u)C(v) \left[ \sum_{x=0}^7 \sum_{y=0}^7 f(x, y) \cdot \cos \frac{(2x+1)u\pi}{16} \cos \frac{(2y+1)v\pi}{16} \right],$$

де  $C(x) = 1/\sqrt{2}$ , коли  $x = 0$  та  $C(x) = 1$  в інших випадках.

$$F^Q(u, v) = \left\lfloor \frac{F(u, v)}{Q(u, v)} \right\rfloor,$$

де  $Q(u, v)$  - 64 елементна таблиця квантування.

До методів приховування інформації у текстових файлах належать:

- синтаксичні методи;
- семантичні методи, які обумовлюють два синоніми, що відповідають значенням прихованих бітів;
- методи довільного інтервалу.

Метод	Знаків стега	Щільність, %
Чергування маркерів кінця	267	0.21
Вирівнювання пробілами	411	0.32
Двійкові нулі	740	0.58
Хвостові пропуски	1071	0.85
Знаки одного накреслення	4065	3.21



Методів приховування інформації в аудіосигналах:

- заміни найменш значущого біта;
- фазового кодування;
- розширення спектру;
- приховування інформації за допомогою вставки тонів;
- приховування інформації використовуючи ехо-сигнал.



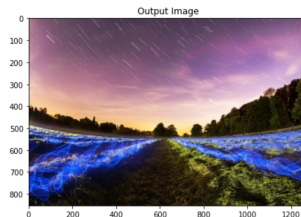
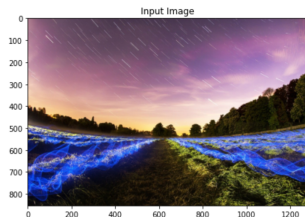
$$IF = 1 - \frac{\sum_{x=1}^n \sum_{y=1}^m (C_{x,y} - S_{x,y})^2}{\sum_{x=1}^n \sum_{y=1}^m (C_{x,y})^2};$$

$$NAD = \frac{\sum_{x=1}^n \sum_{y=1}^m |C_{x,y} - S_{x,y}|}{\sum_{x=1}^n \sum_{y=1}^m |C_{x,y}|};$$

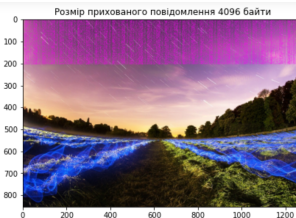
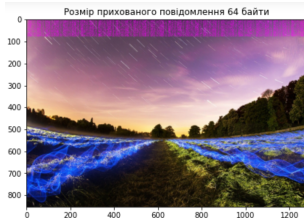
$$SNR = \frac{\sum_{x=1}^n \sum_{y=1}^m (C_{x,y})^2}{\sum_{x=1}^n \sum_{y=1}^m (C_{x,y} - S_{x,y})^2};$$

$$AD = \frac{1}{X \cdot Y} \sum_{x=1}^n \sum_{y=1}^m |C_{x,y} - S_{x,y}|$$

$$MSE = \frac{1}{X \cdot Y} \sum_{x=1}^n \sum_{y=1}^m (C_{x,y} - S_{x,y})^2$$



Розмір повідомлення, байт	MSE	PSNR
64	8.273495506057053e-05	88.95391325528558
128	0.00016699638530676044	85.90373290069535
256	0.00031964390386869873	83.08413934724122
512	0.0006307395466979289	80.13230299219362
1024	0.0012688061742868308	77.09685077517824
4096	0.004987299726455647	71.15214891660129



Розмір зображення: 1280×853

- Стеганографія в поєднанні з криптографією, є потужним захистом інформації.
- Метою стеганографічних алгоритмів є забезпечити приховування факту наявності даних, що потребують захисту.
- Надійними алгоритмами захисту даних в зображеннях є алгоритми маскування та перетворення.
- Найбільш надійним для захисту даних в текстових форматах є метод знаків одного накреслення.
- Для аудіо-форматів найефективнішим вважають метод заміни найменш значущого біта.
- Метод ЗНЗБ для приховування даних в BMP форматі є простим та може приховувати великий об'єм даних.
- Якщо збільшити розмір вбудованих даних, то погіршиться якість зображення.

Дякую за увагу!



<https://github.com/vitalikkk19/Coursework>