ДОДАТОК А
СЛАЙДИ ПРЕЗЕНТАЦІЇ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ
КАФЕДРА ІМІ

МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА
НА ТЕМУ

ЗАХИСТ ДАНИХ СТЕГАНОГРАФІЧНИМИ МЕТОДАМИ НА БАЗІ ВИКОРИСТАННЯ СТРУКТУРНОЇ НАДМІРНОСТІ ОПИСУ КОНТЕЙНЕРІВ

Виконав: Жуков В. В
Керівник: Костромицький А.І.

Харків - 2021

Мета роботи:
дослідження методів маскування даних з використанням мультиконтейнерів для підвищення безпеки даних обмеженого доступу у ході передавання відкритими каналами інфокомунікаційних систем

КЛЮЧОВІ ПИТАННЯ ТА ЗАВДАННЯ МЕТОДІВ СТЕГАНОГРАФІЧНОГО ПРИХОВУВАННЯ ДАНИХ 3

Головні класи завдань, що вирішуються методами стегозахисту інформації:

- забезпечення аутентичності та достовірності даних;
- збереження цілісності даних;
- приховане зберіганням даних, доступ до яких має обмежене коло осіб;
- приховане передавання інформації.

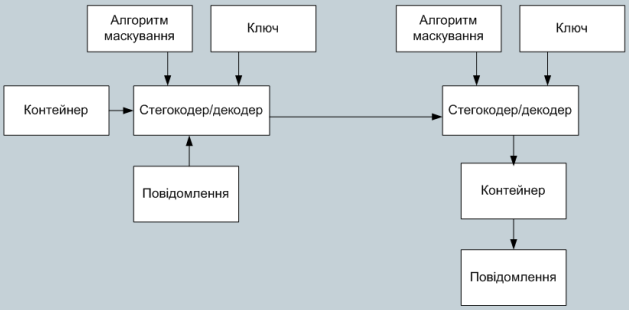


Рисунок 1 – Загальна структурна схема стегосистеми у класичному варіанті побудови

КЛЮЧОВІ ПИТАННЯ ТА ЗАВДАННЯ МЕТОДІВ СТЕГАНОГРАФІЧНОГО ПРИХОВУВАННЯ ДАНИХ 4

Ступінь захищеності стегосистеми:

$$L_p = \frac{\gamma_{um}}{\gamma_m} \times 100\% \quad (1)$$

де γ_{um} - ймовірність викриття повідомлення засобами стегоаналізу, або за участю експерта;

γ_m - ймовірності успішної передачі повідомлення

Відносна ємність стегосистеми:

$$C = \frac{d_m}{d_{all}} \times 100\%. \quad (2)$$

де d_m - відсоток даних прихованого повідомлення;

d_{all} - загальна кількості біт на опис контейнеру

Залежність між захищеністю та ємністю стегосистеми:

$$C \uparrow \rightarrow L_p \downarrow \quad (3)$$

Показник швидкодії алгоритму (скільки біт D може бути оброблено алгоритмом за одиницю часу t роботи):

$$S = \frac{D}{t} = \frac{D}{t_a + t_{tr} + t_b}, \quad (4)$$

де t_a - час підготовчого етапу обробки;

t_{tr} - час на трансформування даних приховуваного повідомлення до вигляду, який може бути вбудовано у контейнер;

t_b - час на вбудовування приховуваних даних у контейнер.

Загальні вимоги до ефективності функціонування стегосистеми:

$$L_p, C, S \rightarrow \max \quad (5)$$

КЛЮЧОВІ ПИТАННЯ ТА ЗАВДАННЯ МЕТОДІВ СТЕГАНОГРАФІЧНОГО ПРИХОВУВАННЯ ДАНИХ 5

Таблиця 1.1 – Відповідність критерії цілісності для деяких файлів поширених типів

Тип файлу	Відповідність критерію цілісності	Примітка
Текстові файли, гіпертекст	+	Пряма інкапсуляція помітно спотворює текстові дані. Тому можливе застосування виключно методів, що вбудовують дані шляхом маніпуляції деякими текстовими параметрами, непомітними спостерігачу (наприклад, змінюють кількість пробілів)
Файли MS Office	-	Після вбудовування даних додатками, які обробляють файли даного типу, файл вважається зруйнованим. Використання у якості контейнеру неможливе
Файли, що можуть виконуванися (exe, cmd, bat)	-	Після вбудовування даних додатками, які обробляють файли даного типу, файл вважається зруйнованим. Використання у якості контейнеру неможливе
Lib, dll, so (файли бібліотек)	-	Після вбудовування даних додатками, які обробляють файли даного типу, файл вважається зруйнованим. Використання у якості контейнеру неможливе
Файли зображень	+++	
Аудіо	+++	
Відеокадри	+++	
Архіви (Zip, 7z, rar)	-	Додустимим є архівація контейнеру. Пряме використання у якості контейнеру файлів даних типів неможливе
Елекронні книги та документи (pdf, fb2, djvu)	-	Контейнером може формуватися з текстового чи графічногофайлу на етапі, що передує його конвертації. Пряме вбудовування даних у файли означених типів неможливе
Системні та конфігураційні файли (sys, reg, ini)	-	Після вбудовування даних додатками, які обробляють файли даного типу, файл вважається зруйнованим. Використання у якості контейнеру неможливе

СТАНДАРТИЗОВАНІ МЕТОДИ ТА АЛГОРИТМИ МАСКУВАННЯ ДАНИХ 6

Використання полів коментаря JPEG

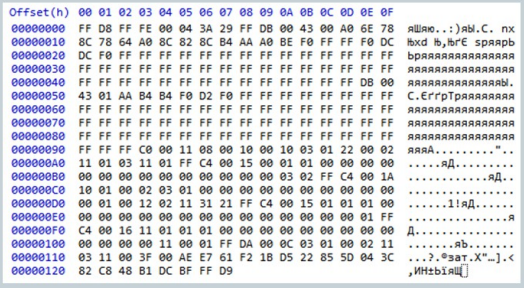


Рисунок 3 – Приклад внутрішньої структури файлу Google favicon.jpg

Рисунок 4 – Зовнішній вигляд файлу Google favicon.jpg

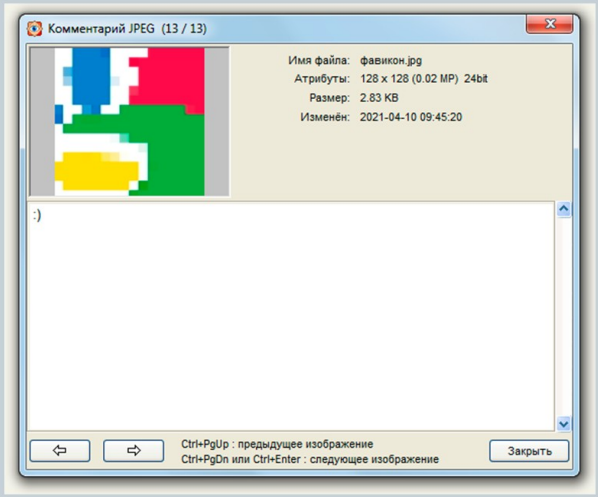


Рисунок 5 – Зчитування JPEG-коментарів за допомогою програмного засобу Fast Stone Image Viewer

СТАНДАРТИЗОВАНІ МЕТОДИ ТА АЛГОРИТМИ МАСКУВАННЯ ДАНИХ

7

Метод останнього біта

Математичний опис процесу модифікації біт LSB:

$$\begin{cases} b(\ell)_{(x,y)} := 0 \mid b'(k)_{(i,j)} = 1 \,\&\, b(\ell)_{(x,y)} = 0 \\ b(\ell)_{(x,y)} := 1 \mid b'(k)_{(i,j)} = 1 \,\&\, b(\ell)_{(x,y)} = 1 \end{cases}, \quad (6)$$

$$\ell = \overline{1;\Lambda},\ k = \overline{1;K}$$

де $b'(k)_{(i,j)}$ - біт секретного повідомлення, який необхідно вбудувати у контейнер шляхом модифікації одного з його LSB-біт;

$b(\ell)_{(x,y)}$ - вихідний біт молодшого розряду.

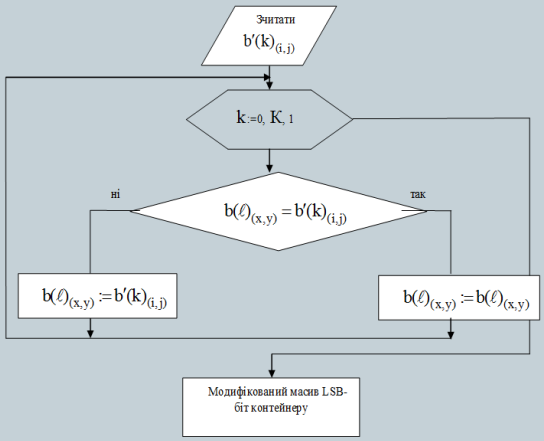


Рисунок 6 – Загальний алгоритм модифікації молодших біт контейнеру на базі LSB-підходу

СТАНДАРТИЗОВАНІ МЕТОДИ ТА АЛГОРИТМИ МАСКУВАННЯ ДАНИХ

8

Метод останнього біта

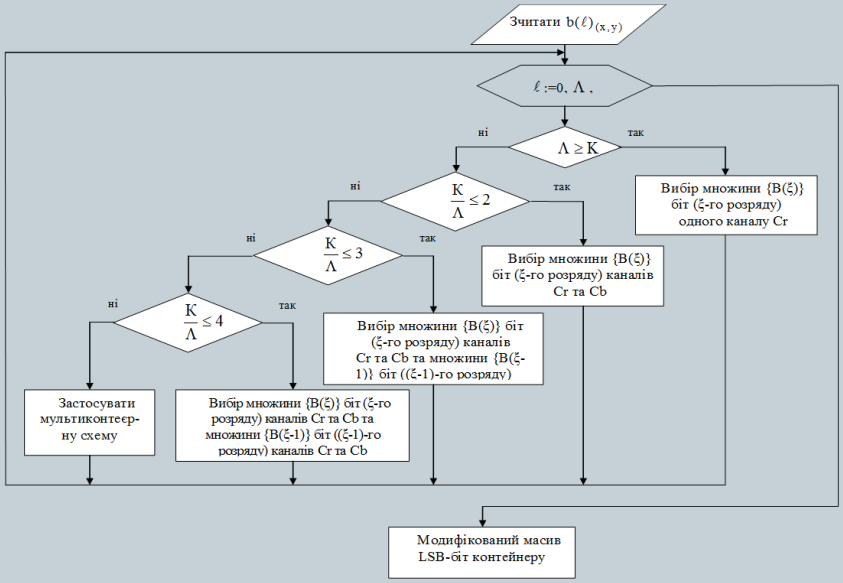


Рисунок 7 – Схема вибору режиму модифікації LSB-біт

СТАНДАРТИЗОВАНІ МЕТОДИ ТА АЛГОРИТМИ МАСКУВАННЯ ДАНИХ 9

Метод останнього біта

Рисунок 8 – Графічний контейнер JPEG (1366x768), що містить частину поеми «Іліада»

Рисунок 9 – Сукупність наймолодших біт графічного контейнеру JPEG виявлена у результаті візуальної атаки

СТАНДАРТИЗОВАНІ МЕТОДИ ТА АЛГОРИТМИ МАСКУВАННЯ ДАНИХ 10

Метод маскування даних на базі дискретного косинусного перетворення

Математичний опис принципу інкапсуляції біт прихованого повідомлення:

$$\begin{cases} \left|\eta(ch)_{x,y}^{(max)}\right| - \left|\eta(ch)_{x,y}^{(min)}\right| > \varepsilon \rightarrow b'(k)_{(i,j)} = 0 \\ \left|\eta(ch)_{x,y}^{(max)}\right| - \left|\eta(ch)_{x,y}^{(min)}\right| < -\varepsilon \rightarrow b'(k)_{(i,j)} = 1 \end{cases}, \quad (7)$$

де $\eta(ch)_{x,y}^{(max)}$ та $\eta(ch)_{x,y}^{(min)}$ - величини максимального та мінімального значень компонент у перетвореному блоці $s_{x,y}$ каналу ch відповідно;

ε - деяка задана величина.

Рисунок 10 – Місце етапу маскування даних на базі дискретного косинусного перетворення у загальному каскаді JPEG-перетворень

СТАНДАРТИЗОВАНІ МЕТОДИ ТА АЛГОРИТМИ МАСКУВАННЯ ДАНИХ 11

Метод маскування даних на базі дискретного косинусного перетворення

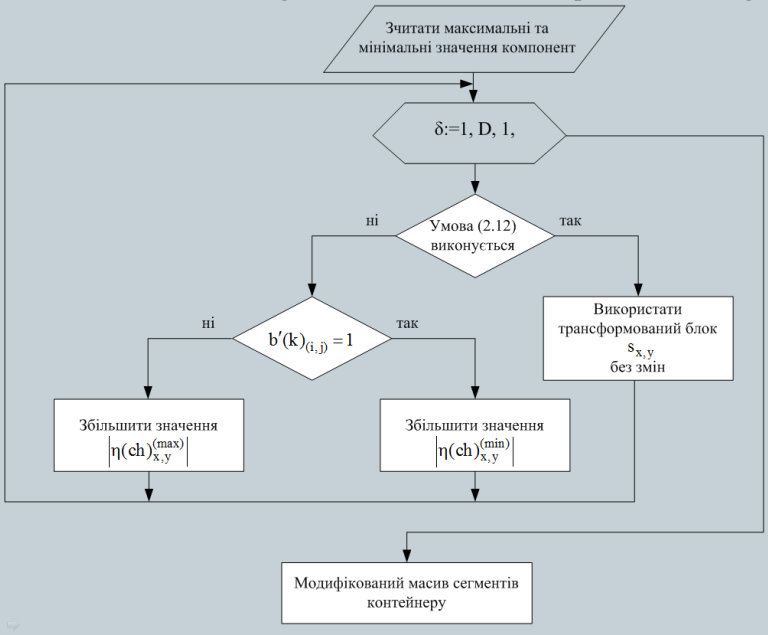


Рисунок 11 – Загальна схема алгоритму вбудовування приховуваних даних на базі дискретного косинусного перетворення за встановленою величиною ε

СТАНДАРТИЗОВАНІ МЕТОДИ ТА АЛГОРИТМИ МАСКУВАННЯ ДАНИХ 12

Метод маскування даних на базі дискретного косинусного перетворення

Рисунок 12 – Приклад візуального спотворення контейнеру

МЕТОД МАСКУВАННЯ ДАНИХ НА БАЗІ ВИКОРИСТАННЯ СТРУКТУРНИХ ОСОБЛИВОСТЕЙ13 ТА НАДМІРНОСТІ СЕГМЕНТІВ ЗОБРАЖЕНЬ

38	29	14	25	6	8	0	0
27	7	9	11	9	0	0	8
21	14	7	0	7	6	0	0
19	10	0	5	0	0	0	0
5	0	0	10	0	0	0	0
11	0	0	0	5	0	0	0
5	5	7	0	0	0	0	0
0	6	6	5	0	0	0	0

- НЧ-область;
- головна діагональ

Рисунок 13 – Приклад блоку після виконання ортогонального перетворення та квантування

а)

б)

Рисунок 14 – Приклад зміни деталізації фрагментів зображення для незначного а) та високого б) рівнів пригнічення ВЧ-складової

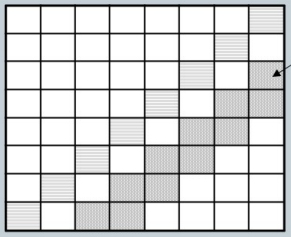


Рисунок 15 – Локалізація ймовірної частотної зони для інкапсулювання біт приховуваного повідомлення

МЕТОД МАСКУВАННЯ ДАНИХ НА БАЗІ ВИКОРИСТАННЯ СТРУКТУРНИХ ОСОБЛИВОСТЕЙ14 ТА НАДМІРНОСТІ СЕГМЕНТІВ ЗОБРАЖЕНЬ

а)

б)

в)

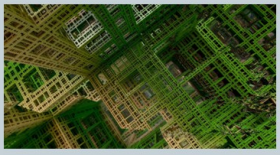


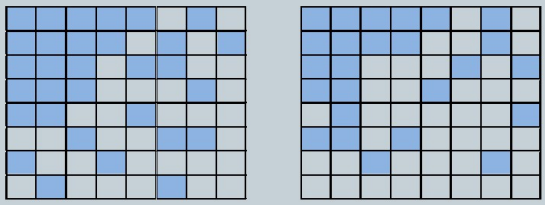
Рисунок 15– Приклади ненасиченого а), середньо насиченого б) та насиченого зображень в)

Показник структурної складності трансформованого фрагменту $s_{x,y}$**:**

$$D_{spctrl} = f(\overline{\ell_i}) = \frac{\sum_{i=1}^{\mu_\ell} \ell_i}{\mu_\ell}, \qquad (12)$$

де ℓ_i - довжина і-ї серії нульових елементів;

μ_ℓ - кількість нульових серій, виявлених у межах трансформованого фрагменту $s_{x,y}$.



а) б)

Рисунок 16 – Приклади трансформованих сегментів різного ступеню структурної складності: високої складності а), для якого $\overline{\ell_i} \approx 2$, та низької складності б) , для якого $\overline{\ell_i} \approx 5{,}5$

МЕТОД МАСКУВАННЯ ДАНИХ НА БАЗІ ВИКОРИСТАННЯ СТРУКТУРНИХ ОСОБЛИВОСТЕЙ ТА НАДМІРНОСТІ СЕГМЕНТІВ ЗОБРАЖЕНЬ 15

Складність фрагменту $s_{x,y}$ у просторовому описі:

$$D_{sptl} = \sum_{x=1}^{8} (p(Y)_{x,y}^{(max)} - p(Y)_{x,y}^{(min)}), \quad (13)$$

де $p(Y)_{x,y}^{(max)}$ та $p(Y)_{x,y}^{(min)}$ - максимальна, та, відповідно, мінімальна величина яскравості пікселя рядка у YCrCb-описі.

Величина динамічного діапазону σ амплітуд компонент у спектральному описі:

$$\sigma = \prod_{i=1}^{10} \left|\eta(ch)_{x,y}^{(i)}\right| - \prod_{j=37}^{64} \left|\eta(ch)_{x,y}^{(j)}\right|, \quad (14)$$

де $\prod_{i=1}^{10} \left|\eta(ch)_{x,y}^{(i)}\right|$ - добудок 10-и модулів НЧ-компонент;

$\prod_{j=37}^{64} \left|\eta(ch)_{x,y}^{(j)}\right|$ - добуток модулів компонент нижче головної діагоналі.

Умови належності сегменту до класу семантично-складних:

$$\left.\begin{array}{c} \sigma \in M_d \ \& D_{sptl} \in P_d \\ \sigma \in M_d \ \& D_{spctrl} \in Q_d \\ \sigma \in M_d \ \& D_{sptl} \in P_d \ \& D_{spctrl} \in Q_d \end{array}\right\} \Rightarrow s_{x,y} \in W, \quad (15)$$

де M_d - множина сегментів, що є складними за показником σ динамічного діапазону амплітуд компонент у спектральному описі;

P_d - множина сегментів, що є складними за показником D_{sptl} складності у просторовому описі;

Q_d - множина сегментів, що є складними за показником D_{spctrl} структурної складності у спектральному представленні.

МЕТОД МАСКУВАННЯ ДАНИХ НА БАЗІ ВИКОРИСТАННЯ СТРУКТУРНИХ ОСОБЛИВОСТЕЙ ТА НАДМІРНОСТІ СЕГМЕНТІВ ЗОБРАЖЕНЬ 16

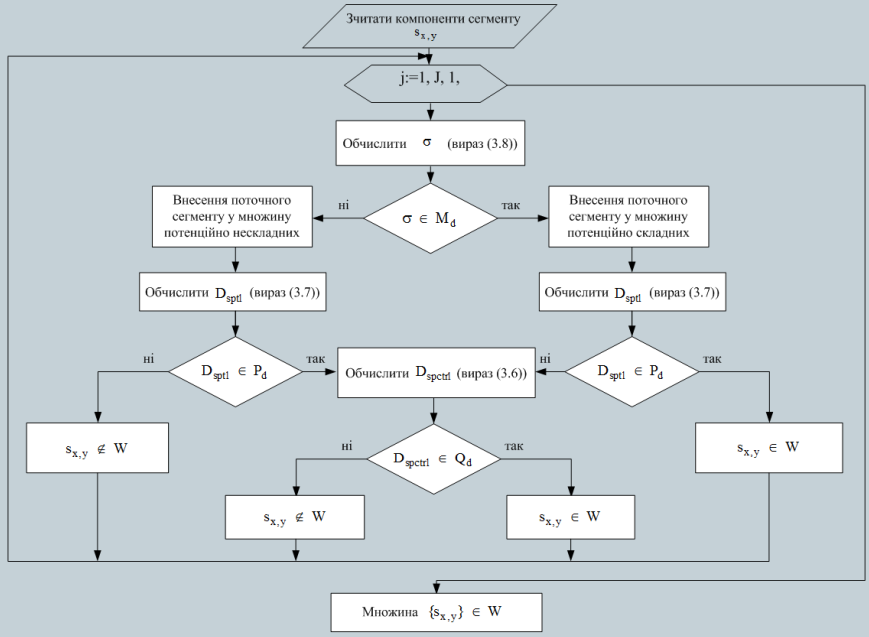


Рисунок 17– Загальна схема визначення належності сегменту до множини семантично-складних

МЕТОД МАСКУВАННЯ ДАНИХ НА БАЗІ ВИКОРИСТАННЯ СТРУКТУРНИХ ОСОБЛИВОСТЕЙ ТА НАДМІРНОСТІ СЕГМЕНТІВ ЗОБРАЖЕНЬ 17

Обчислення розмірності множини компонент, які може бути модифіковано:

$$L_{size} = \text{trunc}\,\frac{g}{s}, \tag{16}$$

де s найчастіше приймається рівним 2.

g - кількість виявлених значущих компонент.

Визначення індексів ψ компонент $\eta(ch)_{x,y}$, що входять до множини L у межах одного сегменту $s_{x,y}$:, та секретного ключа, , який відомий на боці передавача та приймача, тобто:

$$\psi = X(\sigma; D_{sptl}; D_{spctrl}; L_{size}; K) \tag{17}$$

де X - хеш-функція від значень σ, D_{sptl}, D_{spctrl}, та L_{size};

K - секретний ключ.

Принцип нормування компоненти, що віднесено до множини L:

$$\eta'(ch)_{x,y} := v_{th} \tag{18}$$

Принцип модифікації компонент у ході інкапсуляції біт секретного повідомлення:

$$\begin{cases} \eta(ch)_{x,y} := \eta'(ch)_{x,y} - \text{trunc}(0{,}25\eta'(ch)_{x,y}) \mid b'(k)_{(i,j)} = 1 \\ \eta(ch)_{x,y} := \eta'(ch)_{x,y} + \text{trunc}(0{,}25\eta'(ch)_{x,y}) \mid b'(k)_{(i,j)} = 0 \end{cases}, \tag{19}$$

МЕТОД МАСКУВАННЯ ДАНИХ НА БАЗІ ВИКОРИСТАННЯ СТРУКТУРНИХ ОСОБЛИВОСТЕЙ ТА НАДМІРНОСТІ СЕГМЕНТІВ ЗОБРАЖЕНЬ 18

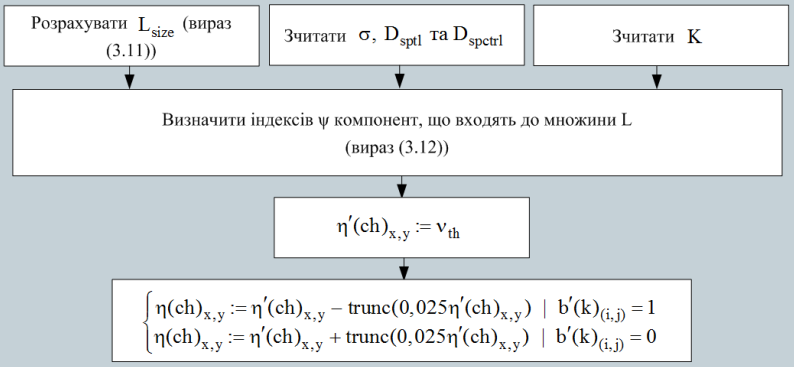


Рисунок 18 - Схематичний опис процесу визначення множини компонент для модифікації та безпосередньо інкапсуляції даних

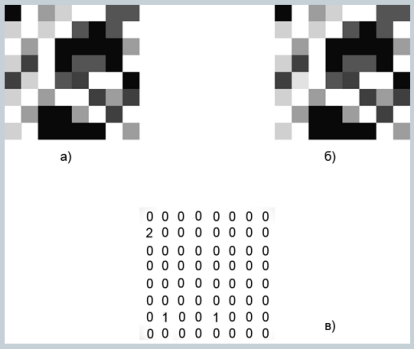


Рисунок 19 - Приклад вихідного сегменту у просторовому представленні а), сегменту, у який було вбудовано 3 біта секретного повідомлення б), матриця абсолютних різниць компонент

ОЦІНКА ПРОДУКТИВНОСТІ МЕТОДУ МАСКУВАННЯ ДАНИХ НА БАЗІ ВИКОРИСТАННЯ СТРУКТУРНИХ ОСОБЛИВОСТЕЙ СЕГМЕНТІВ ЗОБРАЖЕНЬ

Загальна кількість прихованих біт на базі компонент яскравості:

$$R = \frac{H}{8} \times \frac{W}{8} \times L_{size}, \quad (20)$$

де H та W – висота та ширина зображення у пікселях.

Максимальна швидкість передавання біт приховуваного повідомлення у базовому режимі:

$$R(БР)_t = \frac{H}{8} \times \frac{W}{8} \times L_{size} \times n(t)_p \times \nu_{sd} \times \nu_s, \quad (21)$$

де $n(t)_p$ - кількість кадрів P-типу, що буде надіслано за одиницю часу t;

ν_{sd} - коефіцієнт, який показує, яка частина сегментів у кадрі є семантично складними; раніше вказувалося, що $\nu_{sd} = \overline{0,2; 0,8}$;

ν_s - множник, що відображає, який саме розмір у кількості сегментів відносно I-кадру має поточний P-кадр; $\nu_{sd} = \overline{0,8; 0,95}$.

Максимальна швидкість передавання біт приховуваного повідомлення у селективному режимі:

$$R(СР)_t = \frac{H}{8} \times \frac{W}{8} \times L_{size} \times (n(t)_p - 1) \times \nu_{sd} \times \nu_s. \quad (22)$$

Максимальні величини

$R(БР)_t = 32,832$ кБайт.

$R(СР)_t = 21,888$ кБайт

Мінімальні величини

$R(СР)_t = 1,728$ кБайт.

$R(БР)_t = 6,912$ кБайт.

Доповідь закінчено. Дякую за увагу!

Позначення	Найменування	Дод. відомості
	Текстові документи	
1.	Пояснювальна записка	90 с.
	Графічні документи	
2.	Слайди презентації	20
	Інше	

Змін.	Арк.	Номер докум.	Підпис	Дата
Розроб.		Жуков		
Перевір.		Костромицький		
Н. контр.		Костромицький		
Затв.		Безрук		

Захист даних стеганографічними методами на базі використання структурної надмірності опису контейнерів

Відомість атестаційної роботи

Літ.	Аркуш	Аркушів
У	1	1

ХНУРЕ
кафедра ІМІ