Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет *Інфокомунікацій*
(повна назва)
Кафедра *Інформаційно-мережної інженерії*
(повна назва)

# КВАЛІФІКАЦІЙНА РОБОТА
## Пояснювальна записка

рівень вищої освіти другий (магістерський)

*Дослідження можливостей побудови прихованого каналу відео потокового типу на базі існуючих відеосервісів*
(тема)

Виконав:
студент _2_ курсу, групи *ІМІм-22-1*
*Сергієнко М.І.*
(прізвище, ініціали)

Спеціальність *172. Телекомунікації та радіотехніка*
(код і повна назва спеціальності)
Тип програми *освітньо-професійна*
(освітньо-професійна або освітньо-наукова)
Освітня програма *Інформаційно-мережна інженерія*
( повна назва освітньої програми)

Керівник *ст.викл. Твердохліб В.В.*
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ *Безрук В.М.*
(підпис) (прізвище, ініціали)

2024 р.

Не містить відомостей, заборонених
до відкритого публікування

Керівник _____ /*В.В.Твердохліб*

Студент _____ / *М.І. Сергієнко*

Харківський національний університет радіоелектроніки

Факультет *Інфокомунікацій*

Кафедра *Інформаційно-мережної інженерії*

Рівень вищої освіти другий (магістерський)

Спеціальність *172. Телекомунікації та радіотехніка*
(код і повна назва)

Тип програми *Освітньо-професійна*
(освітньо-професійна або освітньо-наукова)

Освітня програма *Інформаційно-мережна інженерія*
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)
«_24_»*жовтня* 2023 р.

# ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові *Сергієнко Марку Ігоровичу*
(прізвище, ім'я, по батькові)

1. Тема роботи *Дослідження можливостей побудови прихованого каналу відео потокового типу на базі існуючих відеосервісів*

затверджена наказом університету від 23 жовтня 2023 р. № 1233 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 24 січня 2024 р.

3. Вихідні дані до роботи *Дослідити можливість побудови прихованого каналу передавання відеоданих з використанням методів стеганографії на базі мультиконтеєрної структури, у ролі якої виступає відеоряд роздільної здатності 1920x1080, 30 кадрів/с при тому, що група включає у себе 8 кадрів. Визначити, за яких умов реалізація такого каналу можлива, а також які параметри матиме прихований відео потік у разі можливості реалізації такого каналу. Забезпечити при цьому максимальну захищеність даних.*

4. Перелік питань, що потрібно опрацювати в роботі *Вступ*
*1 . Архітектура каналів прихованої взаємодії*
*2. Принцип обробки відео даних на базі технологій сімейства MPEG*
*3. Дослідження алгоритмів стеганографічного вбудовування даних*
*4. Оцінка потенційної ємності системи прихованого обміну даними на базі потоку відеокадрів*
*Висновки*

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) _____
*слайди презентації в форматі Power Point (назва та мета роботи, вимоги до систем прихованого передавання даних, структура стеганографічної системи, обсяги відеоконтенту у Всесвітній мережі, особливості обробки кадрів на базі MPEG, огляд стеганографічного методу молодшого біта, оцінка потенційної ємності стегосистеми, висновки)*

**КАЛЕНДАРНИЙ ПЛАН**

| № | Назва етапів роботи | Терміни виконання етапів роботи | Примітка |
|---|---|---|---|
| 1 | Вступ | 24.10.23-26.10.23 | виконано |
| 2 | Архітектура каналів прихованої взаємодії | 27.10.23-8.11.23 | виконано |
| 3 | Принцип обробки відео даних на базі технологій сімейства MPEG | 9.11.23-18.11.23 | виконано |
| 4 | Дослідження алгоритмів стеганографічного вбудовування даних | 19.11.23-27.11.23 | виконано |
| 5 | Оцінка потенційної ємності системи прихованого обміну даними на базі потоку відеокадрів | 28.11.23-16.12.23 | виконано |
| 6 | Висновки | 17.12.23-19.12.23 | виконано |
| 7 | Оформлення пояснювальної записки | 20.12.23-5.1.24 | виконано |

Дата видачі завдання *24 жовтня* 2023 р.

Студент _____
(підпис)

Керівник роботи _____ *ст. викл. Твердохліб В.В.*
(підпис) (посада, прізвище, ініціали)

# РЕФЕРАТ

Пояснювальна записка: 63 с., 23 рис., 22 джерела, 2 додатки

LSB, H.264/AVC, DCT, СТЕГАНОГРАФІЧНИЙ КОНТЕЙНЕР, ГРУПА КАДРІВ, FULLHD

Об'єкт дослідження – стеганографічні механізми, орієнтовані на контейнери графічного типу та відео.

Мета роботи – дослідити потенційні можливості стеганографічних алгоритмів щодо створення прихованого каналу передавання відео.

Виконується дослідження особливостей побудови стеганографічних каналів. Розглядаються закономірності обробки відео у базисі MPEG. Аналізуються механізми вбудовування даних на базі ряду поширених алгоритмів стеганографії. Доводиться теоретична можливість побудови прихованого каналу передавання потокових відеоданих в існуючому технологічному базисі.

# THE ABSTRACT

Explanatory note: 63 p., 23 fig., 22 sources, 2 apps.

LSB, H.264/AVC, DCT, STEGANOGRAPHIC CONTAINER, FRAME GROUP, FULLHD

The object of research is steganographic mechanisms focused on graphic and video containers.

The purpose of the work is to investigate the potential capabilities of steganographic algorithms for creating a hidden video transmission channel.

Research of the steganographic channels construction peculiarities is being carried out. The regularities of video processing in the MPEG base are considered. Data embedding mechanisms based on a number of common steganography algorithms are analyzed. The theoretical possibility of building a hidden channel for streaming video data transmission in the existing technological base is proved.

ЗМІСТ

С.

# ПЕРЕЛІК СКОРОЧЕНЬ

NGFW– (Next Generation Firewall) – міжмережевий екран наступного покоління;
IDS – (Intrusion Detection System) – система виявлення вторгнень;
IPS – (Intrusion Prevention System) – система протидії вторгненням;
APT – (Advanced Persistent Threat) – розвинута стійка загроза;
DPL – (Deep Packet Learning) – глибоке дослідження пакетів, технологія безпеки даних;
PSNR – (Pulse Signal-Noise Rate) – пікове відношення сигнал/шум, показник якості реконструйованих даних;
MSE – (Mean Square Error) – середньоквадратичне відхилення, показник якості реконструйованих даних;
RSA – (Rivest, Shamir, Adeleman) – алгоритм асиметричного шифрування інформації;
HD – (high definition) – відео високої роздільної здатності;
UHD – (ultra-high definition) – відео ультра-високої роздільної здатності;
SD – (small definition) – відео низької роздільної здатності;
H.265/HEVC – (High-Efficiense Video Coding) – технологія кодування відеоданих;
H.264/AVC – (Advanced Video Coding) – технологія кодування відеоданих;
CBR – (Constant Bit Rate) – режим формування/передавання даних з постійною бітовою швидкістю;
JPEG2000 – технологія кодування зображень на базі вейвлетного перетворення;
JPEG – (Joint Pictures Expert Group) – технологія кодування зображень на базі дискретного косинусного перетворення;
BMP – (Bit Map) – формат представлення графічних даних без використання алгоритмів кодування;
RGB – (Red, Green, Blue) – трьохколірна модель;
YCrCb – (Y, Chromatic Red, Chromatic Blue) – яскравісно-хроматична колірна модель;
MPEG – (Motion Pictures Expert Group) – сімейство стандартів відео кодування;
RLE – (Run-Length Encoding) - технологія кодування ланцюжків однакових елементів;

LSB – (Less Significant Bit) – найменш значимий біт;

ДКП – дискретно-косинусне перетворення;

DCT – (Discrete Cosine Transformation) – дискретно-косинусне перетворення.

# ВСТУП

Існуючі реалії сьогодення вимагають від ключових учасників процесів інформаційного обміну надання принципово нових класів послуг на тлі забезпечення послуг вже традиційних форматів.

Одними з таких класів послуг є:

- забезпечення надсилання контенту довільної природи та змісту у режимі «точка-точка» та/або «точка/мультиточка» прихованими каналами;
- виявлення прихованих каналів, несанкціоновано утворених на базі мережевих ресурсів, які надаються, по-перше, провайдерами сервісів а по-друге – провайдерами послуг зв'язку [1-3].

Так, доцільність першого класу послуг зумовлюється постійно зростаючим рівнем кіберзагроз відносно даних з обмеженим доступом у процесі їх обробки, зберігання та надсилання. Зокрема, це є важливим на тлі існуючої тенденції до перевищення темпів виявлення недоліків існуючих механізмів захисту відносно темпів випуску патчів та розробки нових механізмів [2, 4].

У таких умовах ряд механізмів, серед яких – механізми криптографічного захисту даних, а також протоколи безпеки, складовими частинами яких вони є, не можуть гарантувати певний рівень захищеності інформації як наслідок того, що:

- на сьогодні зловмиснику відома більшість недоліків поширених криптосистем;
- зловмиснику сьогодні доступні дуже значні обчислювальні потужності, наприклад, за рахунок використання платформ AWS та подібних; це, у свою чергу, дає змогу досить продуктивної реалізації атак ряду типів, наприклад brootforce [3].

Разом з тим, останнім часом нерідкими є випадки використання алгоритмів побудови прихованих каналів зловмисниками. Це, у свою чергу, несе потенційну небезпеку як кінцевим користувачам, так і провайдерам сервісів, оскільки [3, 4]:

- існує широкий перелік статистичних даних щодо використання прихованих каналів у ході планування та реалізації APT;

- об’єктом APT-атаки може бути провайдер сервісу/зв’язку у випадках, коли надавані ним послуги тим чи іншим чином перешкоджають зловмиснику реалізувати атаку на мережеву інфраструктуру тих чи інших користувачів;
- традиційні засоби моніторингу та протидії зловмисним впливам (IDS/IPS, NGFW, DPL-системи, антивірусні засоби тощо) виявили себе неефективними а у багатьох випадках – взагалі неспроможними протидіяти цільовим атакам з використанням механізмів прихованої передачі.

Таким чином, за даних умов дослідження методів як побудови, так і виявлення прихованих каналів є актуальним науково-практичним питанням.

# 1. АРХІТЕКТУРА КАНАЛІВ ПРИХОВАНОЇ ВЗАЄМОДІЇ

## 1.1 Сутність прихованого обміну даними

Основу прихованої передачі даних становлять стеганографічні методи.

У рамках зазначених методів деяке повідомлення М, що є особливо цінним для усіх учасників процесу обміну даними, до розподіленого середовища спрямовується не самостійно, а попередньо вбудованим до тих чи інших даних [5].

У свою чергу, модуль даних, куди вбудовується приховуване повідомлення, далі являє собою стеганографічний контейнер К.

Процес вбудовування повідомлення М зветься інкапсуляцією.

### 1.1.1 Процедура інкапсуляції даних

У найпростішому випадку, коли процес інкапсуляції здійснюється за принципом «bit per bit», виконується пряма заміна біт $b_i$ контейнеру К бітами $b_m$ повідомлення М відповідно до наступного принципу [5-7]:

$$\begin{cases} b_i := b_i \mid b_m = b_i; \\ b_i := b_m \mid b_m \neq b_i. \end{cases} \tag{1.1}$$

Тобто, за умов рівності значень біт $b_m$ та $b_i$, виконання зміни величин $b_i$ не передбачається.

Таким чином, до каналу надсилається не саме повідомлення М, а деякий контейнер К, який у процесі інкапсуляції було частково змінено за наступним принципом:

$$К' = f(М; К). \tag{1.2}$$

При цьому, для мінімізації викриття факту вбудовування даних, має виконуватися наступна вимога:

$$\Delta К = К - К' \to \min, \tag{1.3}$$

тобто, будь-які відмінності між контейнером К до процесу вбудовування та заповненим К′ повинні бути якомога меншими.

### 1.1.3 Контейнери стенографічних систем. Сутність та загальні вимоги

Залежно від типу даних, до яких належить той чи інший контейнер, показник ΔК може вимірюватися як з об'єктивної, так і суб'єктивної позицій [5, 8].

При цьому, об'єктивна оцінка ΔК може виконуватися лише у випадку, коли аналітик має у розпорядженні вихідний (незаповнений) контейнер К. Тоді для ΔК може оцінюватися за показником пікового відношення сигнал/шум (PSNR), середньоквадратичного відхилення (MSE) та за подібними метриками.

На цей випадок немає потреби навіть виконувати безпосередньо процедуру стеганографічного аналізу.

Звідси може бути сформовано універсальну вимогу до контейнерів – стеганографічний контейнер має бути *глобально унікальним* для того, щоб неможливо було реалізувати, з одного боку, процедуру оцінювання ΔК а з іншого боку – створити умови для неможливості реалізації атаки за відомим контейнером [9].

Водночас, сутність суб'єктивної оцінки зводиться до виявлення тих чи інших типів викривлення змісту контейнеру, конкретика яких визначається його типоналежністю.

У цілому, поняття *контейнер* може розглядатися як на рівні об'єктів 2 та 3 рівня моделі OSI (пакети та кадри), так і на рівні 7, тобто, об'єктів, якими безпосередньо оперують додатки, тобто – файлів.

Водночас, з точки зору раціональності побудови системи прихованого обміну даними, у ролі контейнерів найбільш доцільно розглядати саме файли.

У свою чергу, файл, для того, щоб розглядатися як потенційний стеганографічний контейнер, повинен відповідати ряду вимог, серед яких ключовими є [5]:

1. Поширеність Р у мережі.

Мається на увазі те, що тип даних, а також тип файлу, який може використовуватися як контейнер, у мережі є досить розповсюдженим і його поява не може бути сприйнята, як своєрідна аномалія.

У загальному випадку, дану вимогу щодо поширеності може бути подано, як:

$$P \to \max . \tag{1.4}$$

2. Робастність RC контейнеру.

Відповідність контейнеру К властивості робастності свідчить про те, що навіть за умови втрати, або викривлення деякої кількості біт, які було задіяно для його опису, контейнер все ж продовжує зберігати свою функціональність.

Вимога щодо робастності є у цілому схожою до вимоги поширеності, як показує наступний вираз:

$$RC \to \max \ . \tag{1.5}$$

3. Надлишковість Q контейнеру.

Вимога щодо надмірності контейнеру К може вважатися однією з головних. Сутність її демонструється наступним виразом:

$$Q \to \max , \tag{1.6}$$

інакше кажучи, контейнер мусить мати щонайвищий рівень надмірності.

Під *надмірністю* або *надлишковістю* опису контейнеру мається на увазі його специфічна властивість зберігати свою семантичну цінність та функціональність навіть в умовах, коли певну частину біт, що використовуються для його представлення, змінено довільним чином або взагалі зруйновано.

Вимога щодо рівня надмірності у цілому, з одного боку, є наслідуванням вимогу вимоги (1.5) відносно робастності контейнеру. З іншого боку, сутність даної вимоги додатково пояснюється вимогою щодо ступеню наповненості стеганографічного контейнеру [8], як показує наступна формула:

$$\frac{V_{inc}}{V_c} \to 0 , \tag{1.7}$$

де $V_{inc}$ - кількість даних, інкапсульованих у той чи інший контейнер;

$V_c$ - обсяг біт контейнеру, теоретично доступний для виконання процедури інкапсулювання.

Ця вимога нерозривно пов'язана з вимогою щодо рівня захищеності $\Omega$ стеганограм, що може бути подано у вигляді виразу:

$$\frac{V_{inc}}{V_c} \uparrow \rightarrow \Omega \downarrow . \qquad (1.8)$$

Таким чином, взаємозв'язок вимог (1.6) та (1.7) може бути пояснено тим фактом, що для забезпечення умов для передавання максимально можливого об'єму прихованих даних за одиницю часу, контейнер має характеризуватися максимальним рівнем надмірності.

У цьому випадку навіть тоді, коли величина $V_{inc}$ з виразу (1.7) буде зростати, однак, справедливість співвідношення, між $V_{inc}$ та $V_c$ не буде порушуватися.

## 1.2 Базові компоненти каналу прихованої взаємодії

Незалежно від деталей реалізації та особливостей фізичного середовища надсилання даних, канал прихованої інформаційної взаємодії містить у собі (рис.1.1) [5]:

- модулі інкапсуляції (I);
- модулі декапсуляції (D);
- контейнери прихованого обміну (K).

При цьому, виходячи з особливостей побудови системи прихованого обміну додатковими елементами схеми прихованої інформаційної взаємодії можуть бути:

- криптографічні модулі (C);
- модулі вибору робочого середовища (R).

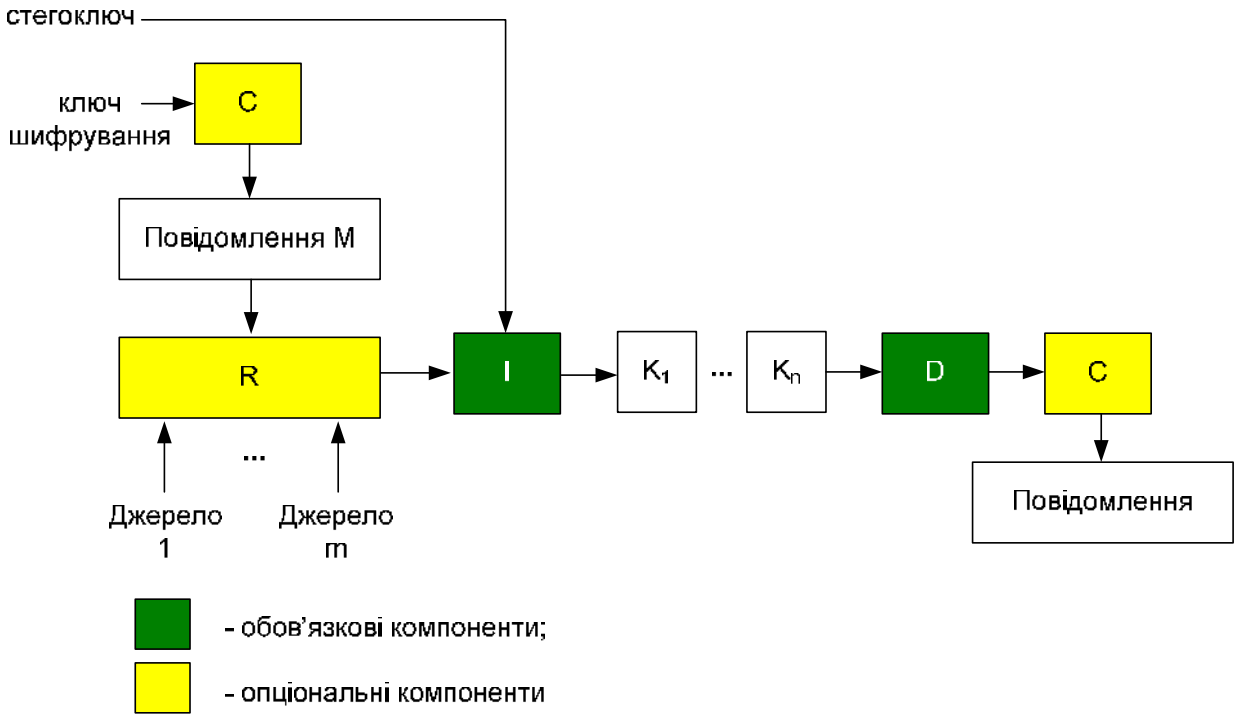



Рисунок 1.1 – Структурна схема каналу прихованої інформаційної взаємодії

У загальному випадку процес функціонування такого каналу може бути описано наступним сценарієм:

1. За умови, що у системі присутній криптографічний модуль, вихідне повідомлення $M$ попередньо зазнає шифрування з використанням того чи іншого криптографічного алгоритму на базі ключа $\xi$ з утворенням шифрограми $M'$, тобто $M' = C(M;\xi)$.

Сутність даної процедури полягає, у першу чергу, в тому, щоб повністю, або хоча б частково зруйнувати семантичні та статистичні характеристики вихідного повідомлення $M$.

Відтак, навіть за найгіршого випадку, тобто, коли ймовірну присутність прихованих даних буде виявлено, за рахунок виконаного шифрування цього процес відновлення масиву $M$ буде максимально забруднено ще на етапі стегоаналізу.

2. Для шифрограми $M'$ повідомлення $M$ (або саме повідомлення у випадку, коли шифрування не виконується) далі за участю модулю $R$ вибору робочого середовища обирається певний інформаційний потік $\theta_i$ з усієї множини потоків $\Theta$, що можуть генеруватися на боці передавача. При

цьому, кожен окремий потік $\theta_i$ - це трафік, що породжується окремими сервісами та додатками які може приймати та передавати вузол.

Кожен потік, може характеризуватися рядом параметрів, зокрема:

- середня інтенсивність $\overline{V(\theta_i)}$ потоку $\theta_i$; даний показник може бути розраховано згідно з наступною формулою:

$$\overline{V(\theta_i)} = \frac{\sum_{j=1}^{J} V_j}{J}, \tag{1.9}$$

де $J$ - кількість часових відліків фіксації бітової швидкості за час спостереження $\tau = \overline{t_1; t_J}$;

$V_j$ - бітова швидкість, що фіксується для кожного $j$-го відліку.

- середній показник часу активності $i-$го джерела, що породжує потік $\theta_i$ відносно часу спокою стосовно процесів як передачі, так і прийому, що визначається за виразом:

-

$$\overline{t_{busy}} = \frac{\sum_{\nu_{tr}=1}^{\nu_{trend}} t_{\nu_{tr}} + \sum_{\nu_{rc}=1}^{\nu_{rccen}} t_{\nu_{rc}}}{\sum_{\nu_{tr}=1}^{\nu_{trend}} t_{\nu_{tr}} + \sum_{\nu_{rc}=1}^{\nu_{rccen}} t_{\nu_{rc}} + \sum_{\nu_{nl}=1}^{\nu_{nlnd}} t_{\nu_{nl}}}, \tag{1.10}$$

де $\sum_{\nu_{tr}=1}^{\nu_{trend}} t_{\nu_{tr}}$, $\sum_{\nu_{rc}=1}^{\nu_{rccen}} t_{\nu_{rc}}$ та $\sum_{\nu_{nl}=1}^{\nu_{nlnd}} t_{\nu_{nl}}$ - сумарний час передавання, приймання даних та спокою відповідно;

- ступінь $\eta_{prop}(\theta_i)$ поширеності типу трафіку, який відповідає потоку $\theta_i$, що може бути подано виразом:

$$\eta_{prop}(\theta_i) \to \max. \tag{1.11}$$

Рішення про вибір певного потоку, при цьому, приймається виходячи з:

- конкретних умов передачі;
- обсягу даних який необхідно передати;

- наявних на вузлі джерел трафіку.

3. Після того, як потік $\theta_i$ обрано, виконується процедура інкапсуляції (вписування) даних повідомлення ($M'$ або $M$) до контейнеру К, або кількох контейнерів $К_i$.

За умови, що у ході надсилання повідомлення прихованим каналом використовується єдиний контейнер К, передача вважається моно контейнерною, якщо ж необхідно задіяти ряд контейнерів $К_i$, мова йде про мультиконтейнерну приховану передачу. У цілому, контейнер являє собою певну складову частину потоку $\theta_i$ [10].

При цьому, потік $\theta_i$ некоректно розглядати, як сукупність з $N$ контейнерів, тобто:

$$\theta_i \neq \bigcup_{i=1}^{N} К_i . \qquad (1.12)$$

Справедливість даного твердження випливає з вимог до стеганографічних контейнерів.

Відтак, лише ті з об’єктів, що задовольняють вимогам виразів (1.4)-(1.7), може бути використано для інкапсуляції даних.

Механізм реалізації процедури інкапсуляції суттєвим чином залежить від використовуваного стеганографічного методу, а також особливостей його реалізації.

Разом з тим, операція інкапсулювання біт повідомлення ($M'$ або $M$) до контейнеру К може зводитися до [5]:

- прямої заміни інформаційних біт $b_i$ контейнеру бітами $b_m$ повідомлення за тим чи іншим законом;
- прямої заміни інформаційних біт $b_i$ контейнеру бітами $b_m$ повідомлення за тим чи іншим законом, але з урахуванням особливостей самого контейнеру;
- непрямої заміни інформаційної складової контейнеру
- прямої заміни службової складової контейнеру;
- опосередкованої заміни службової складової контейнеру;
- запису даних повідомлення до зарезервованих полів контейнеру.

Наближено можна вважати, що пряма заміна тут – це розміщення одного біту повідомлення замість біту контейнеру.

Непряма заміна – така модифікація контейнеру, коли зміна певної множини його біт відповідає вбудовуванню єдиного біта (або кількох біт) повідомлення. І навпаки.

4. Потік даних $\theta_i$ отримується на прийомному боці.

При цьому, маючи у своєму розпорядженні стегоключ $\zeta$, а також сукупність $\{W\}$ інформативних ознак, на базі яких у прийнятому інформаційному потоці $\theta_i$ може бути виокремлено контейнер К (чи масив контейнерів $К_i$), приймач виконує зчитування прийнятого повідомлення $M'$, для чого слугує модуль декапсуляції.

5. Якщо попередньо повідомлення було шифровано, на останньому етапі зворотнього перетворення виконується дешифрування повідомлення з використанням ключа $\xi$ за принципом $M = C(M';\xi)$.

Після цього повідомлення $M$ може бути доступним для цільового додатку користувача.

## 1.3 Регламенти прихованої взаємодії

У цілому, можна виокремити такі базові регламенти побудови процесів віддаленої взаємодії, як [5]:

- синхронна, або безпосередня взаємодія;
- асинхронна, або взаємодія через вузол-посередник.

У першому з зазначених випадків зв'язок двох учасників прихованого інформаційного обміну може виконуватися у реальному часі, як показано рисунком 1.2 а).

У свою чергу, побудова взаємодії асинхронного типу передбачає, що обмін ключами $\xi$ та $\zeta$ може здійснюватися напряму, захищеним каналом (наприклад, шифруючи ключі на базі RSA), тоді як обмін даними потребує наявності хоча б одного транзитного серверу даних (ТСД), як показано на рисунку 1.2 б).

При цьому, вузол-посередник, який може бути використано у ролі ТСД, щонайменше повинен жодним чином не асоціюватися з жодним з учасників прихованої інформаційної взаємодії.

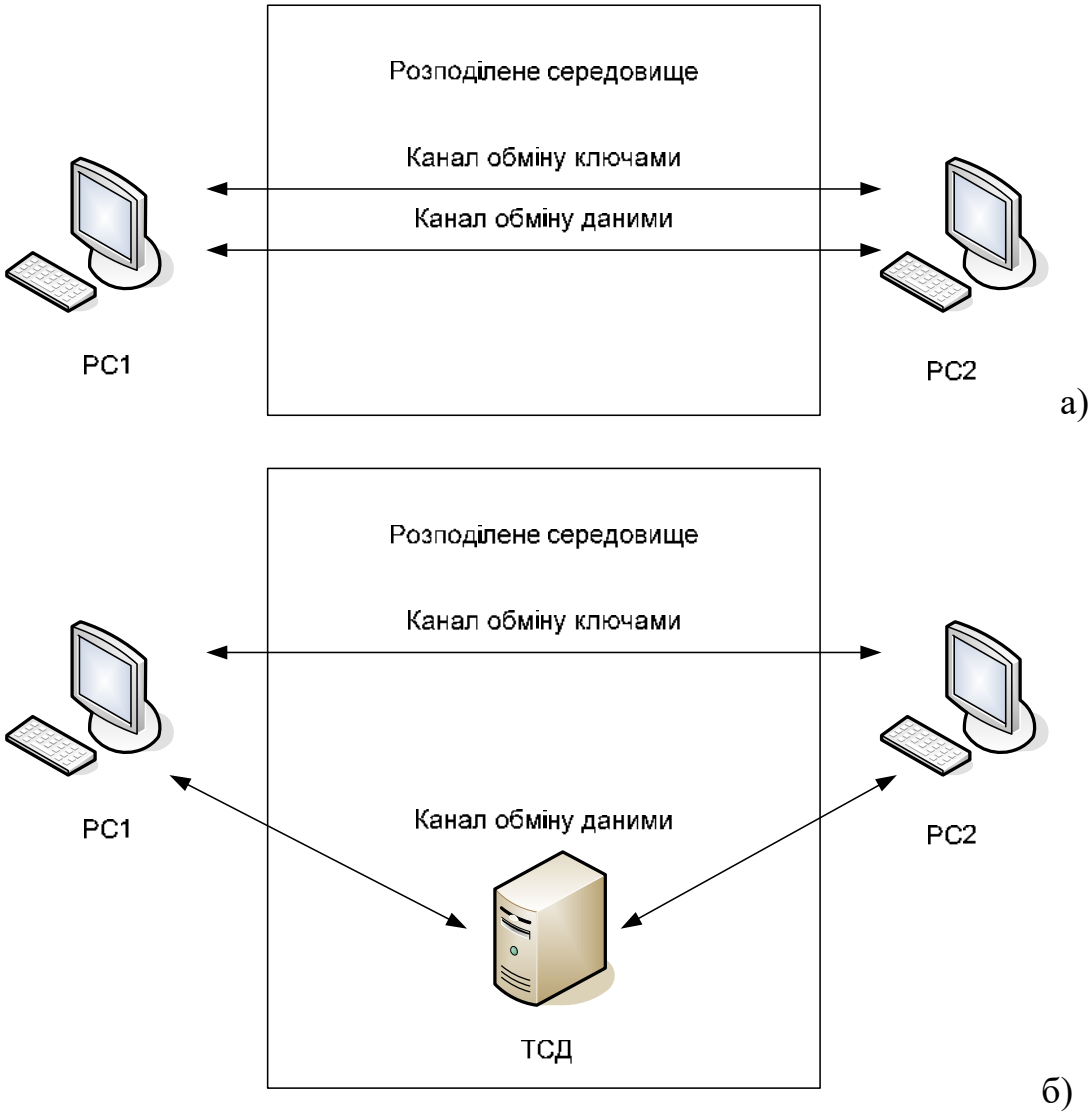



Рисунок 1.2 – Принципи синхронної та асинхронної взаємодії вузлів у ході прихованого обміну даними

Так, ТСД може бути:

- сервер, що забезпечує функціонування одного з мережевих сервісів світового масштабу;
- виділений сервер зберігання даних національного рівня чи регіонального рівня.

Також, теоретично, роль ТСД може виконувати локальний сервер передавача/приймача за умови асоційованості з будь-ким з них (інший провайдер, різні IP тощо). Наприклад, це може бути один зі сторонніх мережевих сервісів зберігання відео (Vimeo, YouTube, Daily Motion, послуги зберігання відео соціальних мереж).

1.4 Огляд типів даних, які може бути використано у ролі стегоконтейнера

Для виявлення типів даних, які можуть використовуватися у ролі контейнерів прихованої інформаційної взаємодії, у першу чергу слід брати до уваги вимоги (1.4)-(1.7). Зокрема, за даними дослідження Cisco VNI Forecast [11], як показано рис. 1.3, домінантним типом даних (за відсотком об'єму) у мережі є відео контент, що цілком задовольняє вимогу (1.4). При цьому, суттєву його частину сьогодні складає відео форматів HD та UHD (рис.1.4).

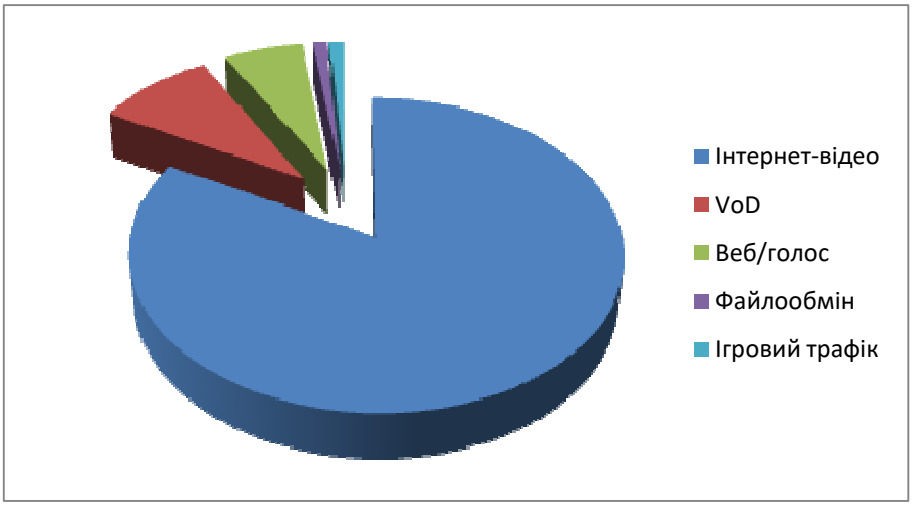



Рисунок 1.3 – Відсоткова частка трафіку різних типів, що розповсюджується Всесвітньою мережею на 2022 рік

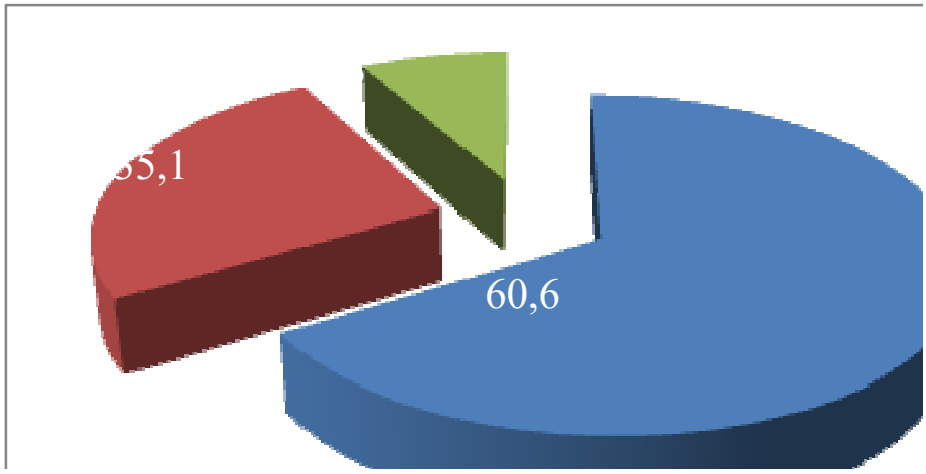



Рисунок 1.4 – Розподіл часток трафіку відео різних роздільних здатностей у Всесвітній мережі станом на 2022 рік

Водночас, спостерігається тенденція до росту UHD-формату на тлі скорочення відсотку SD за у цілому незмінного рівня HD.

Разом з тим, за вимогою (1.5) робастності, у цілому для використання у ролі контейнерів може бути використано будь-які дані, обробка яких передбачає можливість використання методів кодування з втратами. Це такі дані, як [6]:

- аудіо;
- відео;
- графічні.

У свою чергу, говорячи про вимогу щодо надмірності Q контейнеру, поданою формулою (1.6), за аналогією з виразом (1.3) зазначимо, що високий рівень надмірності властивий таким типам даних, для яких справедливим є наступне співвідношення:

$$\Delta V = V - V' \to \max \,|\, RC \approx \text{const}, \tag{1.13}$$

де $V$ - кількість біт, необхідних для опису контейнеру без використання обробки з втратами;

$V'$ - кількість біт, які витрачаються на опис контейнеру за умови, що попередньо було виконано обробку з втратами на найнижчому стандартизованому рівні якості;

$\Delta V$ - абсолютна різниця між величинами $V$ та $V'$ в умовах, коли показник $RC$ робастності не зазнає суттєвих змін.

У свою чергу, за показником $\Delta V$ найбільш пріоритетними типами даних можна вважати:

1. Відео, оскільки сучасні кодеки створюють умови для збільшення величини $\Delta V$. Наприклад, кодек H.265/HEVC може забезпечувати коефіцієнт стиснення на рівні 85-100 [12].

Так, зокрема, для випадку відеоряду, кодованого у даному базисі з роздільною здатністю FullHD (1920x1080), інтенсивність може сягати порядку 7 Мбіт/с, тоді як вихідному відеоряду відповідатиме інтенсивність близько 630-650 Мбіт/с.

При цьому, у даному випадку для кодованого потоку відеоданих забезпечується величина показника пікового відношення сигнал/шум на рівні 35-40 дБ.

Разом з тим, якщо дивитися з позиції суб'єктивного оцінювання, за умови стандартних налаштувань кодеку, візуально помітні викривлення стисненого відеоряду фактично не фіксуються, як це показано на рисунку 1.4.

2. Аудіоряд. Зазначений тип даних також характеризується суттєвими показниками $\Delta V$ .

Наприклад, вихідний аудіоряд у WAV форматі за стандартами CDA генерує потік даних, для якого стандартизований рівень інтенсивності рівняється 1118 Кбіт/с.

Водночас, у випадку його кодування на базі MP3 з опціям за замовчуванням, у режимі CBR буде забезпечено показник інтенсивності рівний 128 Кбіт/с. Тобто, $V$ та $V'$ у даному разі відрізняються між собою майже у 8 разів.

Разом з тим, як свідчать статистичні дані, отримані ще на етапі становлення MP3 [13], понад 90% респондентів не здатні на слух відрізнити вихідні та кодовані аудіодані.

3. Графічна інформація.

На сьогодні один з найбільш поширених форматів графічних даних у мережі є JPEG. Кодек JPEG, при цьому, здатен забезпечити величину коефіцієтна стиснення на рівні 30 значенні при пікового відношення сигнал/шум порядку 35-40 дБ [14].

Менш поширений кодек – JPEG2000 – здатен забезпечити отримання коефіцієнту стиснення до 35 при тих же величинах пікового відношення сигнал/шум.

Стосовно інших типів даних зазначимо, що:

- бінарна інформація (наприклад, скомпільовані дані) та текстовий контент (веб-документи, системні бібліотеки, мета файли тощо) характеризуються виключно такими типами надмірності (кодовою, структурною), що дозволяють застосувати відносно них лише методи кодування без втрат. Це, у свою чергу, дозволяє отримати відносно невисокі показники $\Delta V$ ;

внесення змін у зміст таких файлів у процесі інкапсуляції спричинює незворотну втрату функціональності.


а)


б)

Рисунок 1.3 – Стоп-кадр вихідного відеоряду 1920x1080 а) та відеоряду після кодування (H.265/HEVC, YUV 4:1:1) б)

## 1.5 Попередні висновки щодо аналізу різних типів даних для використання у ролі стеганографічних контейнерів

Виконавши огляд принципу побудови стеганографічної системи, ключових структурних компонент каналу прихованої інформаційної взаємодії та вимог до стеганографічних контейнерів, можна констатувати наступне:

- з позицій вимоги щодо робастності, потенційно прийнятними для застосування у вигляді контейнерів стеганографічних алгоритмів можуть вважатися відео, аудіо та графічні дані;
- з перелічених типів даних у відсотковому вираженні домінантним є відео;
- беручи до уваги величини показника $\Delta V$, беззаперечним лідером можна вважати відеоінформацію;
- відеосередовище дозволяє виконувати передавання даних прихованим каналом як у режимі моноконтейнерів, так і з використанням мультиконтеєрного обміну.

Таким чином, за сукупністю показників в умовах, коли необхідно створити канал прихованої інформаційної взаємодії достатньо високої інтенсивності у реальному часі, теоретично найбільш ефективним типом даних для використання у ролі середовища для формування контейнерів є відеоряд.

Зазначені висновки може біти також підкріплено тим, що:

- якщо не вказано специфічних вимог для функціонування джерела (що має місце у нашому випадку), тоді показником середнього часу активності $i-$го джерела (вираз 1.10) може бути знехтувано;
- показник середньої інтенсивності відео середовища за виразом (1.9) навіть за умови, що на локальних часових ділянках діюча інтенсивність наближатиметься майже до нульової позначки, залишається високим;
- зважаючи на значні обсяги відео контейнерів, кожен з них може бути використано для розміщення відносно великого обсягу біт, не порушуючи справедливість вимоги (1.7).

Отже, для виконання подальшого дослідження можливості побудови каналу прихованої інформаційної взаємодії у реальному часі, попередньо необхідно:

- виконати дослідження існуючих механізмів обробки відеоданих та їх специфіку;
- дослідити поширені алгоритми вбудовування даних у рамках існуючих стегосистем;
- обрати один з зі стеганографічних алгоритмів, керуючись вимогами до захищеності та потенційної ємності;
- розрахувати теоретично можливу інтенсивність передавання даних прихованої інформаційної взаємодії у рамках обраного базису.

# 2. ПРИНЦИП ОБРОБКИ ВІДЕО ДАНИХ НА БАЗІ ТЕХНОЛОГІЙ СІМЕЙСТВА MPEG

## 2.1 Ключові механізми технологій сімейства MPEG

Сьогодні найбільш відомі та поширені технології, що належать до MPEG-групи, це MPEG-2, MPEG-4, H.264/AVC та H.264/HEVC.

Кожна з перелічених технологій виконує обробку відео контенту за двома напрямками [12, 15]:

- на рівні окремого кадру (просторове кодування);
- на рівні потоку (часова обробка).

При цьому, незважаючи на присутність у складі кожної з технологій своїх особливих інструментів та можливостей (різні режими передбачування при обробці окремих кадрів, декомпозиція на сегменти не лише 8x8, але і на 4x4 та 2x2, відмінності у формуванні груп і т.д.), ключовий перелік технологічних етапів обробки є у цілому аналогічним. Це створює умови дял можливості для дослідження базової платформи, без необхідності фокусування на певній її версії.

Виконаємо огляд етапів просторового та часового кодування.

## 2.2 Механізми обробки відеоряду MPEG у часовому форматі

Якщо розглядати відеоряд, як потік відеокадрів $\Psi$, що утворюють структуру динамічної природи, тоді слід зазначити, що головні параметри такого потоку можуть зазнавати змін у певному діапазоні величин, який визначається особливостями його змісту [15].

Зокрема, потік відеокадрів може бути розглянуто як сукупність окремих кадрів $\Psi$, а також існуючих зв’язків між ними, присутність яких та їх характер залежить від особливостей наявного відеоряду (рис.2.1). На даному рисунку показано схему відеопотоку $S$, який утворюється на базі множини груп $G$ кадрів, що послідовно змінюють одна одну з плином часу.

Необхідно зазначити, що протягом одиниці часу $t$ може бути надіслано $F$ кадрів.

У свою чергу, показник F, тобто, частота слідування кадрів, являє собою один з ключових параметрів відеопотоку, поряд зі значенням $G$.

У рамках технологій MPEG, діапазони змін значень як G так і F є жорстко регламентованими.

Так, специфікація H.264/AVC та H.265/HEVC передбачає, що кількість кадрів $\chi$ у складі групи G належить проміжку значень $\chi = \overline{8;\ 32}$ [12].

При цьому, означена специфікація визначає величину для показнику частоти F слідування кадрів на рівні 25 кадрів/с та 30 кадрів/с, як це прийнято для MPEG у цілому.

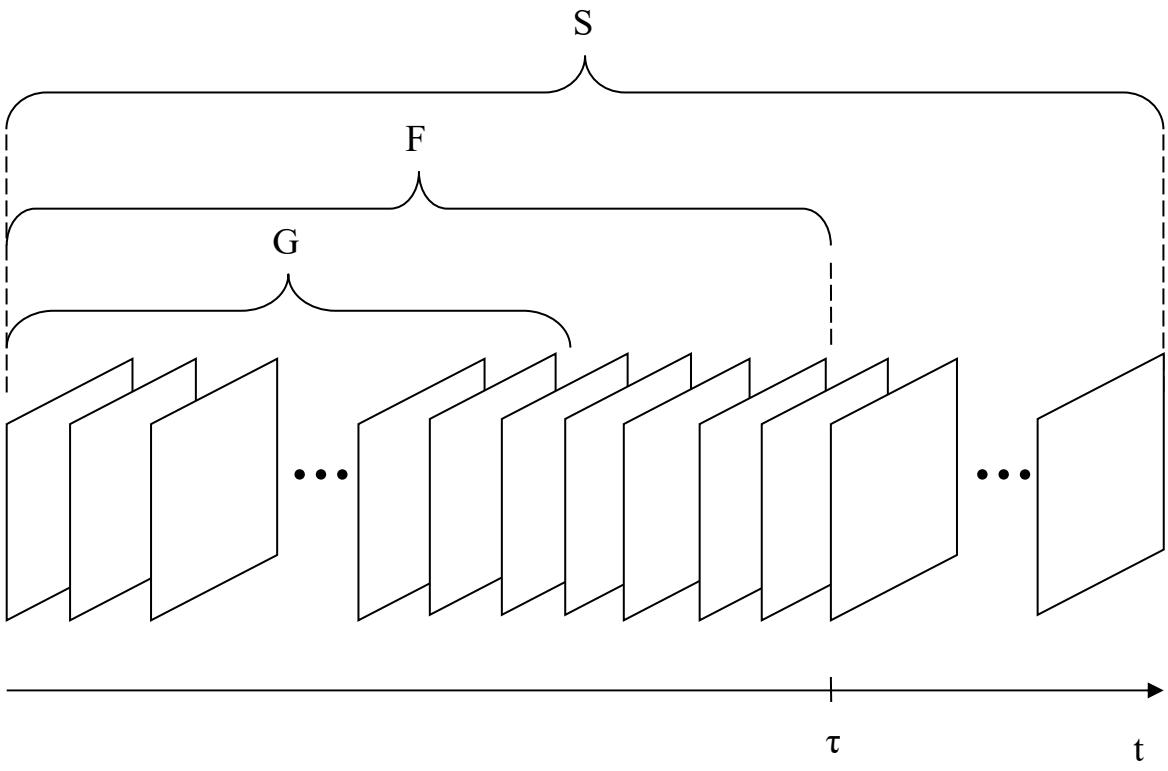



Рисунок 2.1 – Структурна схема формування відеопотоку довільного змісту на базі MPEG

Водночас, номінал величини F має характер рекомендації, так як у той же час немає заборони на генерування відео потоку, для якого значення F може дорівнювати 24, 27 або 28, чи інше наближене число. За великим рахунком, вибір значення параметру F може виконуватися з використанням наступного виразу:

$$F\uparrow \rightarrow V_s\uparrow \,\&\, \Xi\uparrow \,\&\, \vartheta\uparrow, \qquad (2.1)$$

де $\Xi$ - показник, що характеризує візуальну утвореного якість відеоряду;

$\vartheta$ - рівень обчислювального навантаження.

Тобто, ріст величини F веде до збільшення рівня візуальної якості $\Xi$ відеоряду. Водночас, обчислювальне навантаження $\vartheta$ на систему у процесі кодування зростає, при цьому інтенсивність $V_\Psi$ відео у середньому на кадр зазнає скорочення.

Проте, для випадків формату UHD, величина F є жорстко регламентованою. Так, у рамках формату 4K $(4096 \times 3072)$ зазначається вимога до значення F на рівні 60 чи 120 кадрів/с.

У свою чергу, групу G кадрів утворює один базовий (I-кадр) та деяка сукупність зв'язаних кадрів. Тут зв'язаними є т.з. прогнозовані кадри (кадри P-титу - predicted), також кадри, що належать до та двоспрямовано-прогнозованого типу (B-кадри, або bi-predicted кадри) [12, 15].

Використовуючи інформацію, яку містять у собі I-кадр, реалізується процес відновлення змісту кадрів інших типів.

Так, I-кадри містять у собі повну відеосцену, зокрема:

- статичні ділянки – тобто, такі, що за час $t(G)$ не зазнають змін;
- динамічні ділянки.

Кадри I-типу при цьому кодуються повністю.

Разом з тим, P-кадри формуються частково частинами статичних ділянок відеосцени разом з певною множиною векторів руху - ділянок, які зазнають змін протягом часу $t(G)$.

При цьому, формування B-кадрів здійснюється виключно лише на базі векторів руху.

Якщо говорити більш детально, то predicted-кадри (P-кадри) формуються на базі різниці поточного зображення з передуючим базовим кадром або з урахуванням зсувів ряду локальних фрагментів сцени.

У той же час, bi-predicted-кадри (B-кадри) у своєму складі мають лише посилання на передуючий, чи наступний опорний кадр або кадр P-типу з урахуванням зсувів локальних фрагментів.

Базові кадри (кадри I-типу) є базисними компонентами MPEG-потоку. На їх основі може бути реалізовано довільний доступ до якого-завгодно фрагменту відеоряду. При цьому у ході обробки таких кадрів відносно них застосовуються лімітовані рівні стиснення (нижчі, ніж у випадках P та B-кадрів) для того, щоб забезпечити їх візуально високу якість.

У свою чергу, кодування predicted-кадрів виконується відносно передуючих кадрів (I або інших кадрів P-типів) і далі такі кадри застосовуються як порівняльний зразок для наступної послідовності P-кадрів. У цьому випадку може бути забезпечено достатньо високий рівень компресії.

У той же час, найбільш суттєвому стисненню підлягають B-кадри. Так, для того, щоб забезпечити прив'язку кадрів B-типу до відеопослідовності, має використовувати не лише попереднє зображення, але також і наступне зображення [15].

Усередині групи кадрів зв’язки між окремими кадрами, а також порядок їх слідування має жорстке регламентування.

Так, на першій позиції у групі за замовчанням розміщується опорний I-кадр, після якого у деякій регламентованій послідовності з переліку можливих слідують B та P кадри, як зазначено на схемі, поданій рис. 2.2.

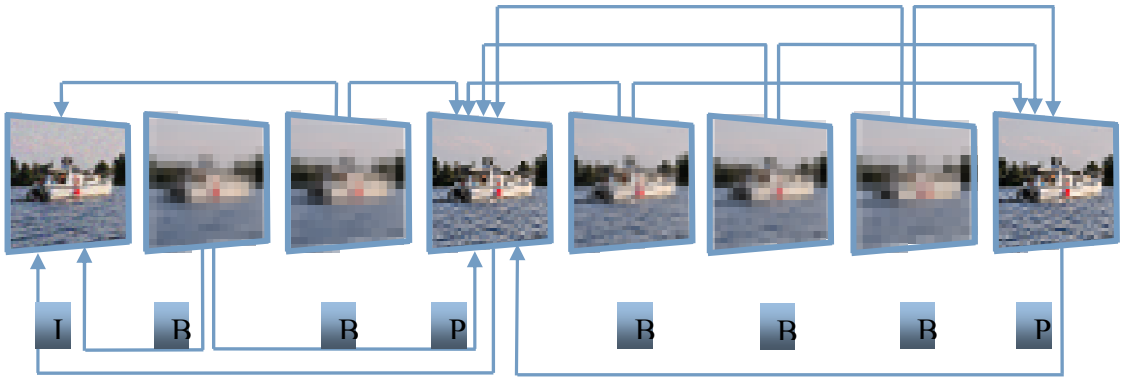



Рисунок 2.1 – Схема формування групи кадрів для розмірності 8

Як свідчать результати аналізу наведеної зв’язності кадрів усередині групи, поданої схемою 2.1, для принципу формування групи властиві такі закономірності:

- формування P-кадрів виконується лише на основі одногоопорного I-кадру, або іншого predicted-кадру;

- зміст кожного з кадрів B-типу визначається даними, що належать двом P-кадрам чи одному P та I-кадру;

- формування B-кадрів на основі інших кадрів B-типу не виконується.

Такі особливості формування у MPEG-потоці кадрів різних типів, у свою чергу, зумовлюють суттєву різницю у кількість біт, що вносяться у групу різними кадрами.

Зрозуміло, що I-кадр здійснює максимальний внесок $V_{(I)}$ у підсумкову бітову швидкість $V_G$ групи. При цьому, середній внесок $\overline{V_{(P)}}$ одного P-кадру у величину $V_G$ поступається $V_{(I)}$, хоча зазвичай є суттєво більшим середньої величини внеску $\overline{V_{(B)}}$ B-кадру.

У свою чергу, сумарну бітова швидкість групи $V_G$ може бути подано наступним виразом:

$$V_G = V_{(I)} + \sum_{j=1}^{J} V_{(P)}^{(j)} + \sum_{k=1}^{K} V_{(B)}^{(k)}, \qquad (2.2)$$

де J та K – обсяг кадрів P та B-типів у групі відповідно.

Наближено вважається, кількість біт $V_{(I)}$, які вносить I-кадр у величину бітової швидкості групи, для переважної більшості випадків складає близько 30-35% від $V_G$ (рис.2.4) [12].

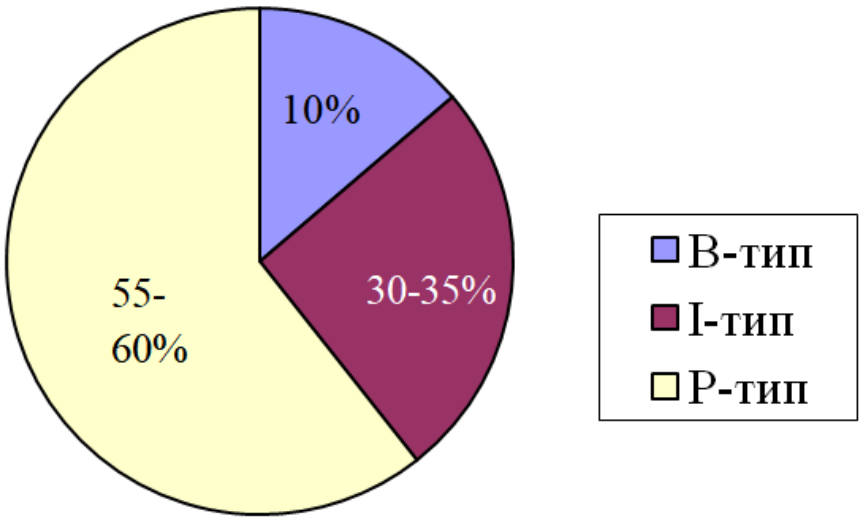



Рисунок 2.2 – Усереднені відсоткові частки вкладів I, P та B кадрів у величину $V_G$ бітову швидкість групи

Означена залежність, у свою чергу, більш детально може пояснити приклад розподілу вкладів у підсумкову бітову швидкість групи G (рис.2.3).

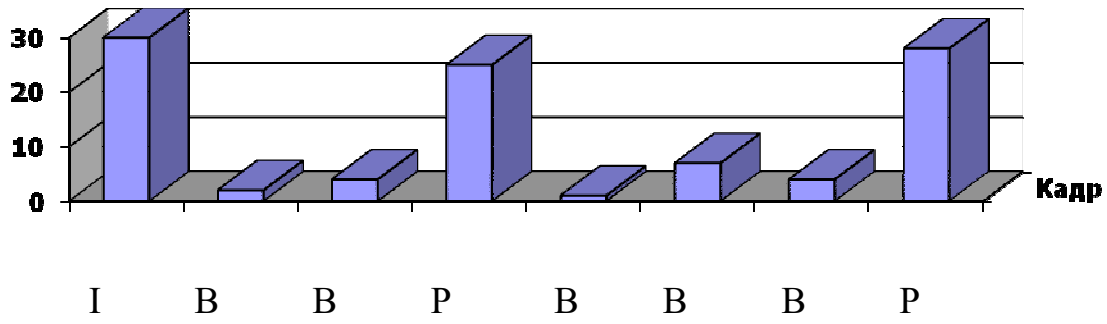



Рисунок 2.3 – Приклад типового розподілу вкладів бітових швидкостей кадрів у групі

Тобто, зазначеним чином, за рахунок побудови відеоряду на базі кадрів, які належать до I, P та B типів, виключаються випадки передавання статичних ділянок відео сцен. Це, у свою чергу, сприяє скороченню інтенсивності відеоряду.

## 2.3 Обробка на рівні окремих кадрів

Загальна обробка кадрів передбачає застосування базисного алгоритму JPEG сукупно з додатковими механізмами (зокрема, просторове передбачення) [13-15].

У свою чергу, ключові технологічні етапи обробки окремого кадру на базі JPEG демонструє рис. 2.4

Так, у ході першого етапу JPEG-обробки реалізується процедура препроцесингу, що зводиться до послідовного виконання:

- операції зміни колірної моделі;
- поділу кадру на сегменти (сегментація, за замовчуванням – 8x8).

У ході операції зміни колірної моделі, здійснюється перехід від композитного формату опису пік селів до яскравісно-хроматичного представлення (ICT - Irreversible Color Transform) [15].

У результаті зазначеної процедури вихідний кадр $\Psi$, попередньо представлений з використанням палітри RGB, отримує опис у просторі YUV

або YCrCb. Кожен піксель при цьому описується на основі трьох компонент, а саме:

- $\sigma(Y)^{(k,\ell)}$, або яскравісна компонента;
- $\sigma(Cr)^{(k,\ell)}$ – хроматична червона компонента (chromatic red);
- $\sigma(Cb)^{(k,\ell)}$ - хроматична синя компонента (chromatic blue,).


Рисунок 2.4 - Загальна схема обробки кадру за алгоритмом JPEG

Необхідність такого перетворення зумовлюється здатністю людського зору дуже чітко відрізняти градації яскравості, тоді як відмінності у колірних відтінках розрізняє значно меншою мірою.

За таких умов використання формату YCrCb дає змогу значно суттєво пригнічувати величини компонент $\sigma(Cr)^{(k,\ell)}$ і $\sigma(Cb)^{(k,\ell)}$, тим самим незворотньо зменшуючи кількість інформації про колірність. При цьому, з одного боку, досягається скорочення початкового об'єму даних а з іншого – візуальні зміни, помітні для людини, у вихідне зображення не вносяться [15].

Зокрема, за замовчуванням використовується формат (4:4:4) колірної субдистретизації. Тобто, спочатку одній компоненті $\sigma(Y)^{(k,\ell)}$ у цьому разі відповідає одна компонента $\sigma(Cr)^{(k,\ell)}$ та одна - $\sigma(Cb)^{(k,\ell)}$. У свою чергу, після переходу до інших форматів, наприклад, (4:2:2), чи (4:1:1) або (4:2:1) кількість хроматичних компонент незворотно скорочується. У зазначений спосіб досягається скорочення до 75% колірної інформації кадру (відповідає моделі 4:1:1).

Схеми зміни формату колірної субдискретизації показано на рис. 2.5.

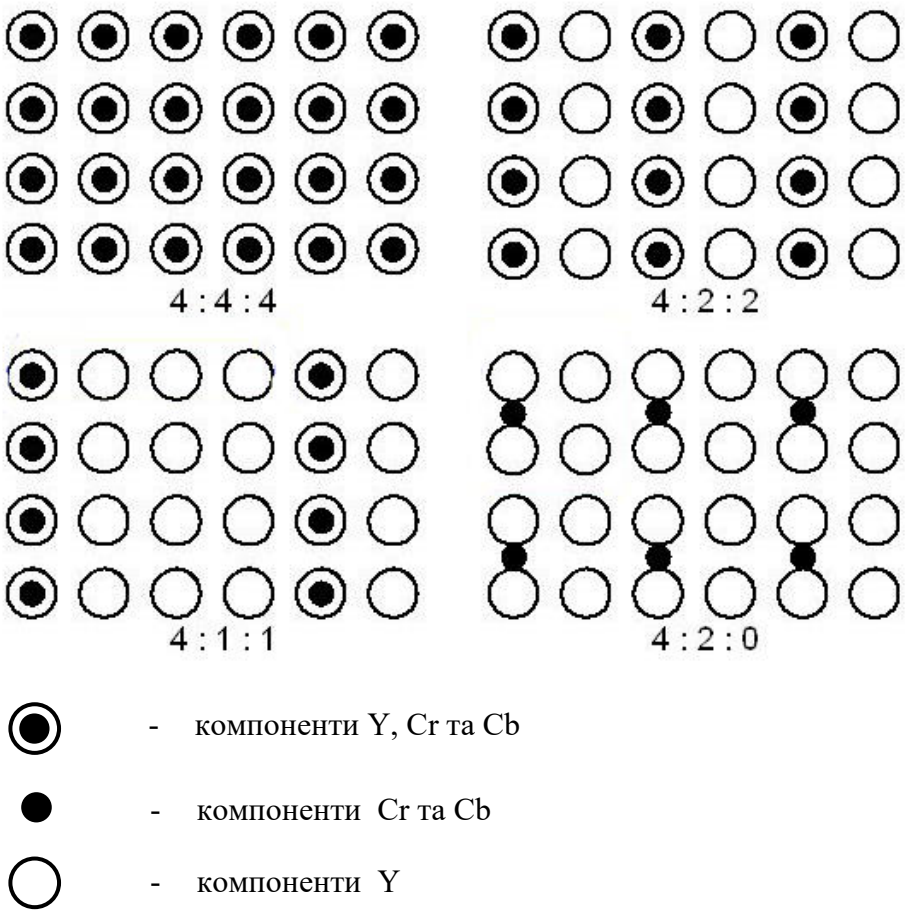



Рисунок 2.5 – Приклади різних форматів колірної субдискретизації

Далі виконується процедура сегментації, після якого обробка кадру $\Psi$ за замовчуванням виконується на рівні сегментів $\psi(\mu)_i$ розміром 8x8, де $\mu$ є індикатором компонентного простору та може приймати значення відповідно Y, Cr чи Cb.

Таким чином, у підсумку формуються три множини сегментів $\psi(Y)_i$, $\psi(Cb)_i$ та $\psi(Cr)_i$ [14].

Наступним кроком обробки сегментів $\psi(Y)_i$ є дискретно-косинусне перетворення (ДКП). У свою чергу, трансформація сегментів $\psi(Cb)_i$ та $\psi(Cr)_i$ виконується з урахуванням різниці передбачених I та P кадрів.

Власне, процедура ДКП не вносить змін у сегменти зображення. Її головне завдання – переведення сегменту $\psi(\mu)_i$ з просторового до спектрального формату опису. У результаті виконання ДКП утворюється сегмент $\psi'(\mu)_i$, у межах якого низькочастотні компоненти позиціонуються у лівому верхньому куті трансформованого сегменту, тоді як компоненти високочастотних компонент – у правому нижньому (рис. 2.6).

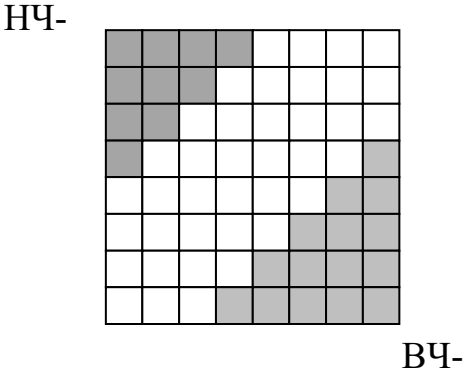



Рисунок 2.6 – Розподіл компонент у сегментові кадру після виконання ДКП за частотною ознакою

Після того, як процедуру ДКП виконано, далі виконується технологічний етап квантування компонент яскравісних та хроматичних компонент. У цьому разі кожна компонента зазнає процедури по елементного ділення на відповідний коефіцієнт матриці квантування.

Далі виконується технологічний етап округлення. За результатом його виконання у зонах високих та середніх частот сегменту $\psi'(\mu)_i$ формується значна кількість ланцюжків нульових біт.

Після цього біти сегменту $\psi'(\mu)_i$ підлягають процедурі зигзаг-сканування (рис. 2.7). Даний технологічний етап забезпечує перетворення двомірної матриці 8x8 сегменту $\psi'(\mu)_i$ на одномірний вектор з 64 елементів.

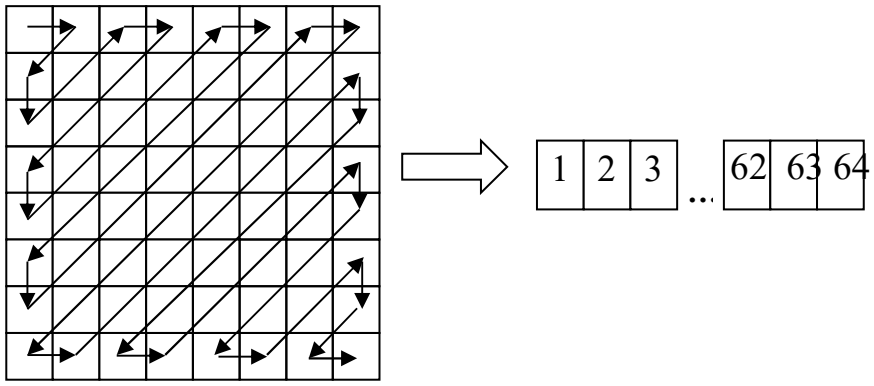



Рисунок 2.7 – Сутність процедури зигзаг-сканування

Сформований 64-елементний вектор, у свою чергу, далі підлягає процедурі кодування на базі алгоритму RLE (run-length encoding). За результатами такої обробки утворюється масив парних елементів вигляду (кількість пропусків, число), у якому у полі «кількість пропусків» вписується лічильником нулів, які необхідно пропустити, тоді як у полі «число» — значення величини, яку слід розмістити у наступній чарунці [13].

Зокрема, у результаті RLE-обробки послідовність 42 3 0 0 0 -2 0 0 0 0 1 може бути подано у вигляді (0,42) (0,3) (3,-2) (4,1).

Заключним етапом обробки даних у базисі JPEG є кодування без втрат на базі MQ-кодеру чи на базі методу Хафмана.

## 2.4 Висновки за результатами аналізу механізмів обробки відеоряду на засадах MPEG

Для розміщення даних секретного повідомлення найбільш прийнятними є кадри B-типу [16].

Це пояснюється тим, що:

- у загальному випадку опису кадрів цього типу як у межах LSB, так і у розрядах більш старших порядків властива наявність високого рівня шуму. Тобто, сама вихідна структура кадрів дозволяє забезпечити більш високі рівні P маскування даних;

- найбільш чутливими до внесення даних є насичені зображення; у свою чергу за самим принципом MPEG кадри B-типу є максимум середньо насиченими;

- для B-кадрів зазвичай застосовуються значно вищі рівні компресії, ніж для кадрів інших типів, це нерідко спричинює виникнення аномалій у міжрозрядному розподілу біт, зокрема, на рівні LSB.

Отже, отримуваний візуальний ефект та особливості статистичного розподілу біт у наслідок модифікування розрядності опису сегментів у загальному випадку не різняться суттєво з відповідними характеристиками пустих контейнерів.

Розглянемо тестову групу G кадрів. Так, I-кадр даної групи наводиться на рис. 2.8.

Водночас, один з кадрів B-типу, які поєднуються у групі G з ключовим I-кадром, демонструється рис. 2.9.

У свою чергу, особливості змісту LSB-простору зазначеного кадру у каналі Cr продемонстровано рисунком 2.10.

Рисунок 2.8 – I-кадр групи G

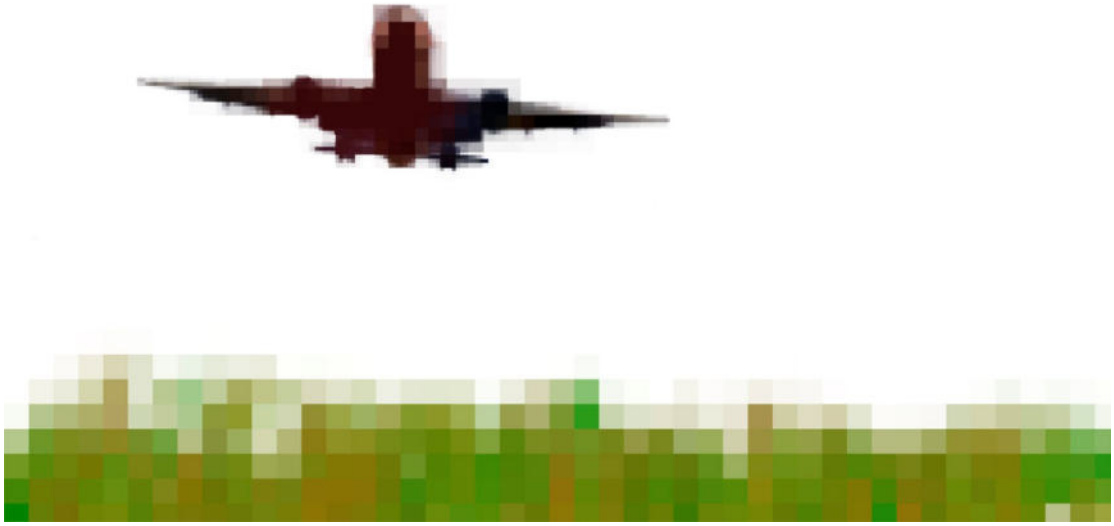


Рисунок 2.9 – Приклад одного з кадрів, що належать до B-типу у складі групи G

Рисунок 2.10 – Зміст LSB-простору каналу Cr B кадру, що належить групі G

Виходячи з зазначеного, можемо констатувати, що знаковою особливістю кадру B-типу є присутність суттєвого обсягу сегментів 8x8, наповнення яких являє собою двійкові елементи, величина яких є рівною (0 або елементи 1) у рамках окремого LSB-каналу компонент – колірно-різницевого, або хроматичного.

Тобто, можна стверджувати, що за деяких умов зазначена специфіка представлення LSB-простору B-кадрів може розглядатися, як природня.

Отже, така особливість представлення LSB кадрів B-типу створює підґрунтя для побудови стеганографічного алгоритму, який потенційно може бути суттєво більш стійким у порівнянні до більшості стандартизованих методів вбудовування секретних даних прямим розміщенням біт.

Беручи до уваги результати аналізу механізмів, які використовуються у ході MPEG-перетворень, а також етапність їх застосування, можна стверджувати, що:

- з точки зору виявлених особливостей внутрішньо кадрової обробки, процедуру інкапсуляції біт повідомлення доцільно виконувати на етапі, що є передуючим по відношенню до етапу кодування без втрат, так як у цьому разі вбудовані дані не буде втрачено у процесі кодування;
- за звичайних умов (обробка типового відеоряду) особливістю представлення кадрів B-типу на рівні як LSB, так і на рівні більш старших розрядів, є присутність помітного рівня шуму. Отже, самі особливості змісту таких кадрів створюють умови для забезпечення потенційно високих рівнів захищеності даних;
- з причини того, що у процесі обробки B-кадрів відносно них застосовуються вищі рівні стиснення, ніж у випадку інших кадрів, це може вести до виникнення аномалій у міжрозрядному розподілу біт, у тому числі, на рівні нульового та інших розрядів; відповідно, візуальний вплив та зміна у характеристиках статистичного розподілу біт за результатами інкапсуляції у загальному випадку не мають помітних відмінностей для випадків пустих та заповнених контейнерів.

# 3. ДОСЛІДЖЕННЯ АЛГОРИТМІВ СТЕГАНОГРАФІЧНОГО ВБУДОВУВАННЯ ДАНИХ

## 3.1 Аналіз механізмів вбудовування інформації

За великим рахунком, незалежно від особливостей реалізації, використовуваних контейнерів та орієнтованість на службову або інформаційну складову потоку-носія, алгоритми стеганографічного вбудовування умовно можна поділити на прямі та непрямі [16, 18].

При цьому очевидно, що з точки зору потенційної ємності більш продуктивними є алгоритми прямі, що ставлять у відповідність одному біту $b_m$ повідомлення M біт $b_i$ контейнеру згідно з принципом, який подано виразом (1.1).

У свою чергу, найбільш поширеним сімейством алгоритмів прямої інкапсуляції, орієнтованих на контейнери графічного типу (BMP, JPEG; кадри відео – як частковий випадок даних, що обробляються на засадах JPEG) сьогодні є LSB. З іншого боку, характерним представником групи алгоритмів, які реалізують принципи опосередкованої інкапсуляції, є метод модифікації DCT-компонент на рівні блоку.

## 3.2 Дослідження методів LSB-групи

### 3.2.1 Вбудовування даних за принципом LSB

В основі LSB-підходу лежить твердження про те, що модифікація молодших розрядів опису пікселя у ході процедури інкапсуляції не веде до виникнення візуально помітних спотворень контейнеру [16, 19-21].

Для того, щоб упевнитися у справедливості даного твердження, розглянемо приклад окремого пікселя до та після модифікації його молодших розрядів.

Нехай $X_{i,j}$ - вихідний піксель у RGB-просторі. У цьому випадку процес побудови його результуючого відтінку вкладами кожного з окремих колірних каналів фактично зводиться до поєднання векторів $X_{i,j}^{(r)}$, $X_{i,j}^{(g)}$ та $X_{i,j}^{(b)}$, де кожен вектор являє собою описом пікселя у окремому колірному просторі. Це еквівалентно представленню пікселя матрицею бінарних

елементів у каналах R, G та B. Така матриця матиме розмірність 3xn, як показано наступним виразом:

$$X_{i,j} = X_{i,j}^{(r)} \,\&\, X_{i,j}^{(g)} \,\&\, X_{i,j}^{(b)} = \begin{vmatrix} 2^{n-1} & 2^{n-2} & \dots & 2^{\mu} & \dots & 2^{2} & 2^{1} & 2^{0} \\ 2^{n-1} & 2^{n-2} & \dots & 2^{\mu} & \dots & 2^{2} & 2^{1} & 2^{0} \\ 2^{n-1} & 2^{n-2} & \dots & 2^{\mu} & \dots & 2^{2} & 2^{1} & 2^{0} \end{vmatrix}, \quad (3.1)$$

де $\mu = \overline{0;\ n-1}$ - кількість розрядів, необхідних для представлення пікселя у кожному з трьох каналів;

$X_{i,j}^{(r)}$, $X_{i,j}^{(g)}$ та $X_{i,j}^{(b)}$ - вектори колірного опису пікселя на базі RGB.

У свою чергу, графічно даний принцип може бути проілюстровано рисунком 3.1.

$X_{i,j}$

| | | |
|---|---|---|
| $b(7)_{i,j,1}$ | $b(7)_{i,j,2}$ | $b(7)_{i,j,3}$ |
| $b(6)_{i,j,1}$ | $b(6)_{i,j,2}$ | $b(6)_{i,j,3}$ |
| $b(5)_{i,j,1}$ | $b(5)_{i,j,2}$ | $b(5)_{i,j,3}$ |
| $b(4)_{i,j,1}$ | $b(4)_{i,j,2}$ | $b(4)_{i,j,3}$ |
| $b(3)_{i,j,1}$ | $b(3)_{i,j,2}$ | $b(3)_{i,j,3}$ |
| $b(2)_{i,j,1}$ | $b(2)_{i,j,2}$ | $b(2)_{i,j,3}$ |
| $b(1)_{i,j,1}$ | $b(1)_{i,j,2}$ | $b(1)_{i,j,3}$ |
| $b(0)_{i,j,1}$ | $b(0)_{i,j,2}$ | $b(0)_{i,j,3}$ |
| R | G | B |

- одиничний біт

Рисунок 3.1 – Принцип, за яким формується колірне значення пікселя на базі RGB

На рисунку 3.1 наведено приклад пікселя $X_{i,j}$, який сформовано на базі біт трьох колірних каналів – R, G та B відповідно. Значення пікселя у двійковому форматі дорівнює 101001011000110010100010.

При цьому, біти, що знаходяться на 8, 16 та 24 позиції бінарного представлення, для даного випадку формують простір найменш значущих біт (LSB) – по одному на канал R, G та B.

Відповідно до засад LSB-стеганографії, модифікації у ході процедури інкапсулювання зазнають найменш значущі біти одного чи кількох каналів [8, 10, 18, 19].

Окрім цього, за певних особливостей змісту контейнеру додатково, окрім біт LSB-простору, біти повідомлення може також бути вбудовано у сусідні розряди (щонайменше – у перший). У цих умовах, з одного боку, зростає загальна ємність а з іншого – може зменшуватися ємність вбудовуваних даних.

Сам процедура інкапсуляції має такі властивості:

- множина біт, на базі якої здійснюється опис вихідного файлу, що використовується у ролі контейнеру, кількісно дорівнює множині біт заповненого файлу-контейнеру (тобто, такого, який містить у собі приховане повідомлення);

- значення біту $b_i$ файлу-контейнеру у випадку, коли його значення початково дорівнює біту $b_m$ повідомлення, який вбудовується, не зазнає змін.

Далі розглянемо випадок модифікації пікселя, показаного на рисунку 3.1. У ході процедури інкапсуляції виконується запис числа 7 (або 111 у двійковому форматі) у його бінарну форму представлення. За результатами такої модифікації отримуємо послідовність біт 10100101100011011010001**1**. У свою чергу, у зазначеній послідовності виділені символи відповідають вбудованим бітам.

Тепер дослідимо інший випадок, коли для інкапсуляції на рівні пікселя використано не лише LSB-розряд, але і розряд, наступний після нього (перший). При цьому, у даний піксель вбудовується число 63 (або 111111 у бінарному представленні). У цих умовах вихідне, а також отримані після інкапсулювання візуальні представлення пікселя будуть такими, як зображається рисунком 3.2.

а) б) в)

Рисунок 3.2 – Колірні відтінки початкового пікселю а), після модифікації одного б) та двох LSB-розрядів в)

З аналізу рисунку 3.2 можемо зробити висновок, що візуальні відмінності у розглянутих зразках відсутні. Таким чином, модифікація LSB-біт не вносить викривлень у контейнери.

3.2.2 Аналіз механізму заповнення контейнеру

Сукупність біт розряду LSB (або будь-якого іншого) формує бітову площину $\Phi_\mu$, тобто:

$$\Phi_\mu = \bigcup_{m=1}^{H} \bigcup_{n=1}^{W} b(\mu)_i^{(m,n)}, \qquad (3.2)$$

де $b(\mu)_i^{(m,n)}$ - біт $\mu$-го розряду з координатами $(m,n)$ у зображенні;

$i$ - індекс біту у суцільній нумерації.

У свою чергу, класична реалізація методу LSB передбачає можливість інкапсулювання біт $b_m$ повідомлення у площину $\Phi_0$ (LSB) а за необхідності – площину $\Phi_1$ (першого розряду) в усьому діапазоні значень координат $(m,n)$ та з можливість суцільного заповнення як усього доступного простору контейнеру (що визначається величиною V), так і його певних частин.

Зазначений спосіб реалізації LSB може бути пояснено наступним алгоритмом:

1. Встановити послідовність обходу контейнеру.
2. Встановити початкову координату вбудовування.
3. Зчитати біт $b_i$.
4. Виконати порівняння значень $b_m$ та $b_i$.
5. Якщо величини $b_m$ та $b_i$ рівні, $b_i$ залишається незмінним, інакше – його значення інвертується.

6. Перевірити ознаку кінця повідомлення.

7. Якщо кінця повідомлення не досягнуто, зчитати біт $b_{m+1}$, інакше – завершити процедуру.

8. Перевірити ознаку кінця контейнеру.

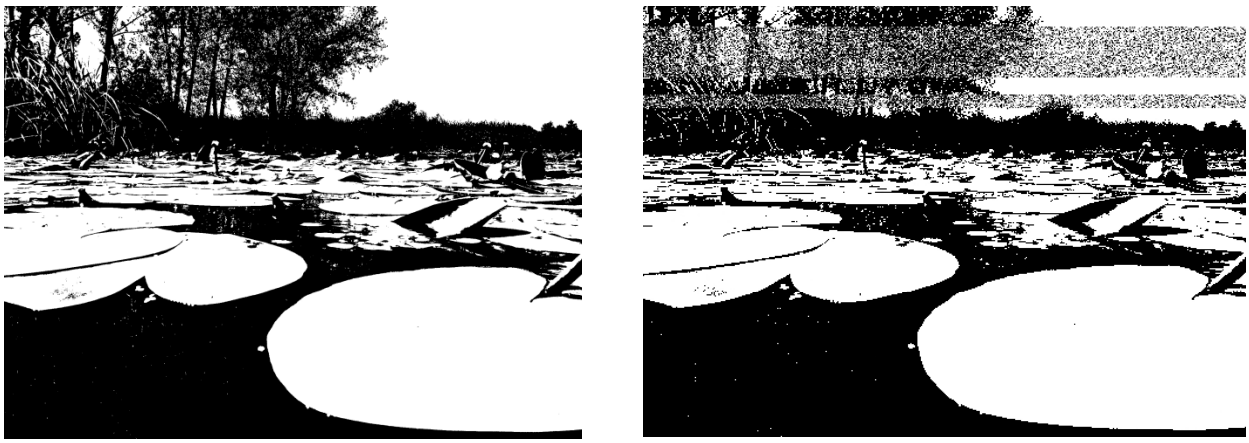
9. Якщо кінця контейнеру не досягнуто, зчитати біт $b_{i+1}$, інакше – обрати наступний контейнер.

10. Перейти до кроку 4.

Таким чином, для даного способу заповнення контейнеру важливою є лише кількість $V_m$ біт повідомлення M та доступна ємність ($V_c$ або $V_{inc}$) самого контейнеру.

При цьому, орієнтування на величину $V_{inc}$ сприяє збільшенню захищеності $\Omega$ вбудованих даних, як свідчить вираз (1.8) [21].

Разом з тим, такий спосіб, у разі його класичної реалізації, цілком ігнорує особливості змісту площини контейнеру. Це веде до появи структурних аномалій площини $\Phi_0$, які може бути легко виявлено, виконавши декомпозицію заповненого контейнеру до рівня множини $\Phi_\mu$ та далі проаналізувавши зміст $\Phi_0$ (рис.3.3).



а) б)

Рисунок 3.3 – LSB-зміст незаповненого а) та заповненого б) контейнеру

У свою чергу, адаптивні механізми заповнення контейнеру забезпечують виконання інкапсуляції біт $b_m$ у структурно складні ділянки простору LSB зображення. Це можуть бути або контурні ділянки, або фрагменти, що містять природне шумоподібне заповнення (рис. 3.4) [8].

Рисунок 3.4 – Ділянки, що містять шумоподібне заповнення та контури

Як можна бачити з розміщеного прикладу, візуальний аналіз зразку не свідчить про наявність вбудованої інформації. Тобто, захищеність таких даних є значно вищою.

Таким чином, перевагою класичної реалізації є можливість забезпечення значної ємності $V_{inc}$ при тому, що вимога (1.8) буде виконуватися. Якщо орієнтуватися виключно на вимогу технічного завдання щодо даної величини, то зазначений спосіб можна вважати прийнятним.

Проте, враховуючи уразливість даного способу заповнення контейнеру до візуального аналізу, його застосування не є доцільним.

Тому, з дочки зору забезпечення балансу між значеннями ємності $V_{inc}$ та захищеності, у рамках LSB найбільш ефективним можна вважати побудову стегоканалу на базі одного з адаптивних алгоритмів.

При цьому, для створення умов збільшення доступної ємності $V_{inc}$, доцільно використовувати зображення високої насиченості, що характеризуються великою кількістю контурних ділянок та фактурних фрагментів.

На випадок, коли мультиконтейнерною структурою є відеоряд, необхідно його обирати таким чином, щоб забезпечувалася висока динаміка змін сцен.

## 3.3 Дослідження методів, орієнтованих на модифікацію DCT-компонент на рівні блоку

### 3.3.1 Аналіз механізму вбудовування даних

Методи даної групи, як і LSB, частіше за все використовують у якості контейнерів JPEG-зображення [19].

При цьому, як і для LSB, етап вбудовування даних реалізується після виконання процедури округлення (рис.3.5).

На першому кроці методу вимірюється різниця абсолютних значень $\left|\sigma^{(k,\ell)}\right|$ компонент у межах трансформованого блоку $\psi'(ch)_i$.

Якщо така різниця буде більшою, ніж деяка величина $\varepsilon$, вважається, що зазначений блок $\psi'(ch)_i$ виконує передачу символу 0.

Інакше, коли така різниця є меншою, ніж деяке значення $(-\varepsilon)$, тоді має передаватися 1.

Зазначений принцип демонструється наступним виразом:

$$\begin{cases} \left|\sigma_{max}^{(k,\ell)}\right| - \left|\sigma_{min}^{(k,\ell)}\right| > \varepsilon \rightarrow b_m = 0; \\ \left|\sigma_{max}^{(k,\ell)}\right| - \left|\sigma_{min}^{(k,\ell)}\right| < -\varepsilon \rightarrow b_m = 1, \end{cases} \quad (3.3)$$

де $\sigma_{max}^{(k,\ell)}$ та $\sigma_{min}^{(k,\ell)}$ - найбільша та найменша величини компонент у межах сегменту $\psi'(ch)_i$ каналу ch відповідно.

Разом з тим, оскільки характер розподілу значення величини $\varepsilon$ як на рівні кадру.

Так, відповідно, і на рівні окремих сегментів є довільним, для можливості реалізації процесу вбудовування біт $b_m$ секретного повідомлення за принципом (3.3), необхідно спочатку налагодити процес зміни величини $\varepsilon$ згідно з до законом зміни самого повідомлення.

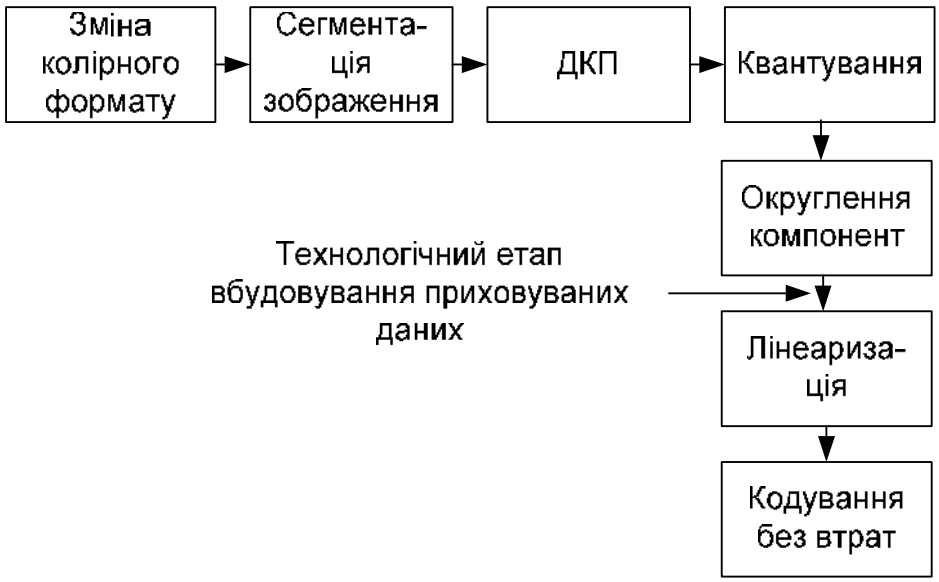



Рисунок 3.5 – Включення етапу інкапсуляції в узагальнену схему JPEG-перетворень

Отже, очевидним є те, що контейнер може зазнавати модифікацій на рівні сегментів $\psi'(\mathrm{ch})_i$. Тому для того, щоб мінімізувати візуальні та статистичні викривлення, що вносяться при цьому, доцільно виконувати модифікацію величин компонент лише у каналах Cr та Cb, так як внесення змін у канал Y може вести до помітних викривлень [19].

У свою чергу, умову необхідності попередньої зміни значень $\sigma_{\max}^{(k,\ell)}$ та $\sigma_{\min}^{(k,\ell)}$ може бути подано співвідношенням:

$$\begin{cases} \left|\sigma_{\max}^{(k,\ell)}\right| - \left|\sigma_{\min}^{(k,\ell)}\right| < \varepsilon \\ \left|\sigma_{\max}^{(k,\ell)}\right| - \left|\sigma_{\min}^{(k,\ell)}\right| > -\varepsilon \end{cases} \tag{3.4}$$

Тоді у випадку, коли умова (3.4) для сегменту $\psi'(\mathrm{ch})_i$ є справедливою, відповідно, значення $\sigma_{\max}^{(k,\ell)}$ та $\sigma_{\min}^{(k,\ell)}$ має бути від кореговано, змінивши їх на величину $\Delta\sigma$, яка обчислюється за наступним виразом:

$$\Delta\sigma = \varepsilon - \left|\sigma_{\max}^{(k,\ell)}\right| - \left|\sigma_{\min}^{(k,\ell)}\right|. \tag{3.5}$$

Реалізація процесу інкапсуляції передбачає можливість розгалуження загального сценарію виконання у випадках, коли:

- необхідно виконати корегування або - $\sigma_{max}^{(k,\ell)}$ або $\sigma_{min}^{(k,\ell)}$;

- корегується як $\sigma_{max}^{(k,\ell)}$, так і $\sigma_{min}^{(k,\ell)}$.

При цьому, ураховуючи специфіку JPEG-обробки, можемо зазначити, що зміна величини $\sigma_{max}^{(k,\ell)}$ вище певної порогової, яка, у свою чергу, визначається змістовними особливостями самого сегменту, веде до виникнення суттєвих візуальних спотворень.

Для уникнення подібних ситуацій більш доцільним є  доцільним є виконання корекції  величини компоненти $\sigma_{min}^{(k,\ell)}$, що відповідає ВЧ-складовій сегменту $\psi'(ch)_i$. Така закономірність зумовлена тим, що зміна величин ВЧ-компонент (так само, як і виключення з опису сегменту деякої їх множини) не спричинює виникненню помітних візуальних викривлень контейнеру.

У той же час, корекція значення $\sigma_{min}^{(k,\ell)}$ виконується у випадках, коли необхідно вбудувати у контейнер елементу «1», тоді як інкапсуляція символу «0» передбачає (у випадку потреби) корегування значення компоненти $\sigma_{max}^{(k,\ell)}$.

Відтак, для скорочення ймовірності виникнення візуальних за результатами вбудовування даних, у якості контейнеру використовуються зображення JPEG, які характеризуються високою насиченістю.

### 3.3.2 Дослідження механізму заповнення контейнеру

На відміну від базисних методів LSB, даний метод не передбачає прямої інкапсуляції біт повідомлення. Це, у свою чергу, дозволяє уникнути недоліків, властивих попередньо розглянутому методу. Зокрема [8, 20]:

- відсутні візуальні аномалії у просторі наймолодших біт;
- відсутні зміни статистичних характеристик сегменту, які може бути виявлено існуючими алгоритмами стегоаналізу.

Отже, за таких умов біти $b_m$ повідомлення можуть вбудовуватися у ході прямого обходу контейнеру, під час якого дані опосередковано інкапсулюються у кожен сегмент $\psi'(ch)_i$ зображення. При цьому, відмінності у реалізації методу можуть різнитися лише способом та напрямком обходу (рис.3.6).

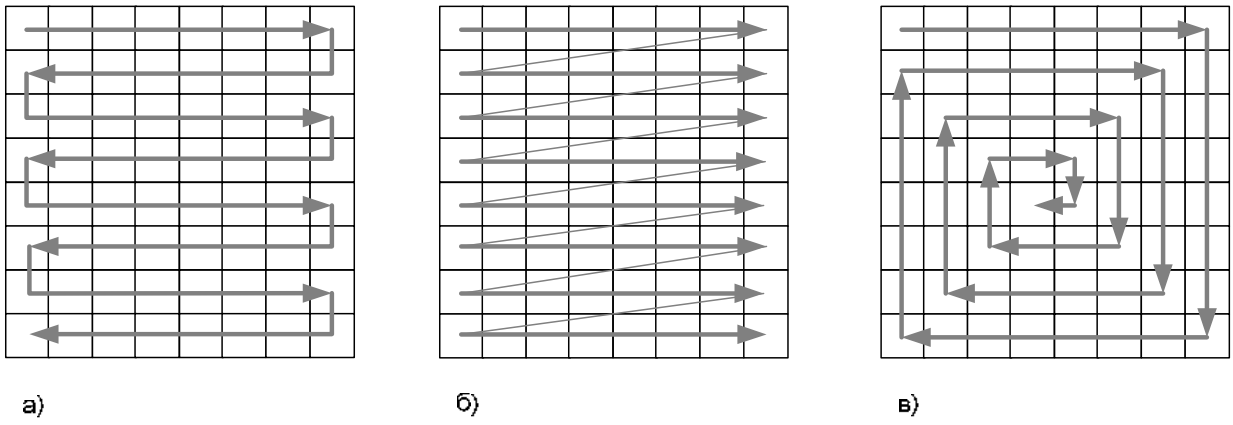



Рисунок 3.6 – Прикладки напрямків обходу кадру: лінійний а), горизонтальний б), «равлик» в)

Отже, якщо одному сегментові $\psi'(ch)_i$ зображення відповідає один вбудований біт $b_m$ повідомлення M, тоді загальний об'єм даних, вбудованих зазначеним способом, може бути розраховано за виразом:

$$V = \frac{HW}{64}. \tag{3.6}$$

Звідси виходить, що кадр 1920x1080 у випадку, коли для інкапсуляції використовуються усі сегменти $\psi'(Cr)_i$ - хроматичного синього каналу – величина становитиме $V = 32400$ біт. У свою чергу, на базі двох каналів Cr та Cb можемо отримати сумарно $V = 64800$ біт.

Разом з тим, на практиці важко знайти контейнер, який у випадку використання усіх його сегментів не зазнає візуально помітних змін, що проявляються, зокрема, на:

- градієнтних ділянках;
- ділянках одного тону;
- ділянках, що містять елементи, що мають закономірності повторень.

З цієї причини для того, щоб уникнути спотворень контейнеру, заповнюється його незначна частина, яка складає зазвичай 10-20% обсягу сегментів. Тобто, 3240-6480 для випадку кадру FullHD.

Саме тому сьогодні методи даної групи частіше за все використовуються для внесення водяних знаків у зображення. Інше використання їх обмежене.

Таким чином, за показниками захищеності даних та ємності найбільш доцільним для побудови каналу прихованого обміну даними високої інтенсивності є адаптивні LSB-методи.

# 4. ОЦІНКА ПОТЕНЦІЙНОЇ ЄМНОСТІ СИСТЕМИ ПРИХОВАНОГО ОБМІНУ ДАНИМИ НА БАЗІ ПОТОКУ ВІДЕОКАДРІВ

## 4.1 Умови оцінювання потенційної ємності системи прихованого обміну даними

Раніше було виявлено, що інтенсивність відеоряду, сформований на базі MPEG, є величиною, змінною у часі з причини, по-перше, специфіки побудови а по-друге – з причини того, що відео, за визначенням, є інформаційною структурою, що динамічно змінюється з часом. У свою чергу, це є наслідком динаміки змісту відео сцен. Також попередньо було обґрунтовано вибір B-кадрів потоку, як елементів мультиконтеєрної структури.

Виходячи з зазначеного, а також ураховуючи діаграму 2.3, очевидно, що для послідовності з N кадрів B-типу справедливою є наступна залежність:

$$HW_{B_1} \neq HW_{B_2} \neq ... \neq HW_{B_i} \neq ... \neq HW_{B_N} \ , \qquad (4.1)$$

де H та W – відповідно, висота та ширина кадру.

При цьому, на рівні довільної групи $G_j$ різниця між $HW_{B_i}^{(max)}$ та $HW_{B_i}^{(min)}$ може сягати як значення $HW_{B_i}^{(max)} - HW_{B_i}^{(min)} \approx HW_{B_i}^{(max)}$, так і $HW_{B_i}^{(max)} - HW_{B_i}^{(min)} \approx 0$, що суттєво утруднює розрахунки [12].

Таким чином для того, щоб мати можливість формалізації процесу розрахунку доступної ємності, оцінка виконується на тлі припущення про те, що середня розмірність B-кадру складає 10% від загальної роздільної здатності кадру. Для урахування цього буде використано множник $\varepsilon = 0{,}1$ [8].

Оцінка ємності при цьому виконується для випадку, коли алгоритмом інкапсуляції є LSB, в умовах:

- максимального заповнення контейнеру (класична реалізація LSB);

- заповнення контейнеру з забезпеченням максимальної захищеності вбудованих даних (адаптивні алгоритми);
- застосування різних форматів колірної субдискретизації.

Водночас, обчислення ємності динамічної мультиконтеєрної структури виконується для випадків максимальної та мінімальної довжин груп у прив'язці до часового інтервалу 1 сек.

Також, за умовами завдання, розрахунок виконується для відеоряду з роздільною здатністю 1920x1080.

## 4.2 Розрахунок ємностей для випадку моноконтейнеру

### 4.2.1 Оцінка ємності контейнеру без попередньої внутрішньо кадрової обробки

Стеганографічні механізми, які застосовуються для вбудовування даних у JPEG-контейнер, виконують модифікацію його спектрального опису – тобто, модифікація контейнеру виконується на рівні компонент ДКП, після здійснення процедур квантування та округлення.

При цьому, зазначене перетворення здійснюється окремо для компонент яскравості $\sigma(Y)^{(k,\ell)}$ та хроматичних - $\sigma(Cb)^{(k,\ell)}$ та $\sigma(Cr)^{(k,\ell)}$, що використовуються для опису кадру замість композитних каналів RGB вихідної палітри [13-15].

До того ж, виходячи з встановлених опцій, які кодек використовує у ході обробки, одній компоненті $\sigma(Y)^{(k,\ell)}$ у відповідність може ставитися як одна компонента $\sigma(Cr)^{(k,\ell)}$ і одна - $\sigma(Cb)^{(k,\ell)}$ (формат 4:4:4), так і значно менша кількість колірно-різницевих компонент.

Якщо розглядати випадок модифікації контейнеру у просторовій області (що відповідає розгляду файлу BMP у ролі контейнера), на базі палітри RGB, на цей випадок потенційно доступний обсяг біт $V_{rgb}$ для інкапсуляції (теоретично можлива ємність стегосистеми у перерахунку на один контейнер) може бути розрахована наступним чином [10]:

$$V_{rgb} = 3HW\mu, \qquad (4.1)$$

де $\mu$ - обсяг розрядів, які може бути задіяно для вбудовування біт повідомлення.

Наприклад, якщо будемо розглядати випадок повної модифікації одного розряду (нульового за замовчуванням) у каналах R, G, та B, тоді для кадру відео формату HD (1980x1080) згідно з формулою (4.1) отримуємо $V_{rgb} = 3 \times 1920 \times 1080 \times 1 = 6,33$ Мбіт, або 0,74 МБ.

Отриманий показник, який є справедливим для випадку безпосередньої модифікації даних для файлу BMP-типу, є максимальним у рамках сімейства алгоритмів LSB.

Відповідно, для випадку заповнення одного каналу, доступний обсяг біт $V_{ch}$ дорівнюватиме 2,11 Мбіт ($\approx 0,25$ МБ).

Разом з тим, так як механізми обробки MPEG за замовчуванням орієнтуються на обробку яскравісно-хроматичного простору компонент, говорити про ємність B-кадру на цей випадок немає сенсу.

### 4.2.2 Оцінка ємності контейнеру на базі JPEG

Виконаємо спочатку розрахунок теоретично можливої ємності окремого контейнеру. Водночас, на випадок розгляду контейнеру формату JPEG, формулу (4.1) необхідно актуалізувати та представити у наступній інтерпретації [10]:

$$V^{(YCrCb)} = (H_Y W_Y + H_{Cr} W_{Cr} + H_{Cb} W_{Cb})\mu, \qquad (4.2)$$

де $H_Y$ та $W_Y$ - значення висоти та ширини простору компонент яскравості відповідно;

$H_{Cr}$ та $W_{Cr}$ - значення висоти та ширини простору хроматичних червоних компонент відповідно;

$H_{Cb}$ та $W_{Cb}$ - значення висоти та ширини простору хроматичних синіх компонент відповідно.

Разом з тим, є очевидним той факт, що розмірність просторів хроматичних компонент залежить від обраних налаштувань кодеку, а саме – встановленого режиму колірної субдискретизації. Так, у випадку застосування формату 4:4:4, підсумкова ємність стегосистеми у перерахунку

на кадр дорівнюватиме також $V_{4:4:4}^{(YCrCb)} = 3 \times 1920 \times 1080 \times 1 = 6,33$ Мбіт (0,74 МБ).

Завважимо, що тут говориться про обсяг біт після декомпресії, які потенційно може бути вбудовано. Також, у даному разі не береться до уваги скорочення об'єму даних після виконання процедури ентропійного кодування.

Відтак, для B-кадру, ураховуючи множник $\varepsilon$, вираз (4.2) може бути доповнено до вигляду:

$$V_{4:4:4}^{(YCrCb)} = (H_Y W_Y + H_{Cr} W_{Cr} + H_{Cb} W_{Cb}) \mu \varepsilon . \qquad (4.3)$$

Тоді отримуємо $V(B)_{4:4:4}^{(YCrCb)} = 0,1 V_{4:4:4}^{(YCrCb)} = 0,633$ Мбіт (0,074 МБ).

При цьому, якщо буде застосовано інший формат колірної субдискретизації, тоді обсяг біт хроматичних просторів, які може бути модифіковано, відповідно, зміниться.

Наприклад, якщо розглядати режим 4:1:1, зазначимо, що кожна колірно-різницева площина буде являти собою простір, вчетверо менший від вихідного. Відтак, у цьому разі маємо $V_{4:1:1}^{(YCrCb)} = (1920 \times 1080 + \frac{1920 \times 1080}{4} + \frac{1920 \times 1080}{4} \times 1) = 3,1$ Мбіт, або, 0,37 МБ. Тобто, це вдвічі менше від початкового значення, що відповідає формату 4:4:4. Для B-кадру у цьому випадку максимальна ємність дорівнюватиме $V(B)_{4:1:1}^{(YCrCb)} = 0,1 V_{4:1:1}^{(YCrCb)} = 0,31$ Мбіт (0,037 МБ).

У свою чергу, для розрахунку можливого рівня заповненості контейнеру з забезпеченням максимальної захищеності вбудованих даних на базі адаптивних алгоритмів, необхідно взяти до уваги вираз (1.7), за яким обсяг $V_{inc}$ вбудованих біт має бути величиною, суттєво меншою, ніж загальна доступна ємність. Припустимо, що захищений об'єм складає 10% від доступного.

За таких умов у межах одного B-кадру може бути вбудовано $\widehat{V}(B)_{4:4:4}^{(YCrCb)} = 0,0633$ Мбіт (0,0074 МБ) для формату 4:4:4.

При цьому, для формату 4:1:1, відповідно, маємо $\widehat{V}(B)_{4:1:1}^{(YCrCb)} = 0,1 V_{4:1:1}^{(YCrCb)} = 0,031$ Мбіт (0,0037 МБ).

Також, якщо розглянути випадок, коли простором для інкапсуляції є виключно площина компонент $\sigma(Y)^{(k,\ell)}$, тоді з виразу (4.2) виключаються складові, які ураховували множини компонент $\sigma(Cr)^{(k,\ell)}$ та $\sigma(Cb)^{(k,\ell)}$, тобто:

$$V^{(Y)} = H_Y W_Y \mu . \tag{4.4}$$

Таким чином, якщо говорити про загальну ємність контейнеру у даних умовах, тоді $V^{(Y)} = 1920 \times 1080 \times 1 \approx 2{,}07$ Мбіт (0,26 МБ).

Відтак, для контейнеру на базі B-кадру отримуємо $V(B)^{(Y)} = 0{,}1V(B)^{(Y)} = 1920 \times 1080 \times 0{,}1 \approx 0{,}207$ Мбіт (0,026 МБ)

Водночас, на випадок забезпеченням максимальної захищеності вбудованих даних, маємо $\hat{V}(B)^{(Y)} = 0{,}1\, V(B)^{(Y)} \approx 0{,}0207$ Мбіт (0,0026 МБ).

## 4.3 Оцінка ємності мультиконтейнерної структури

Виконаємо спочатку розрахунок максимально можливої ємності.

У загальному випадку, оскільки розрахунок обсягу вбудованих біт для випадку мультиконтейнерного ряду виконується для інтервалу часу 1 сек, для формату 4:4:4 його може буди реалізовано на базі наступного виразу:

$$V(t)_{4:4:4}^{(YCrCb)} = (H_Y W_Y + H_{Cr} W_{Cr} + H_{Cb} W_{Cb})\mu\beta\varepsilon , \tag{4.5}$$

де $\beta$ - частота надходження B-кадрів;

тоді як для формату 4:1:1:

$$V(t)_{4:1:1}^{(YCrCb)} = (H_Y W_Y + \frac{H_{Cr} W_{Cr}}{4} + \frac{H_{Cb} W_{Cb}}{4})\mu\beta\varepsilon . \tag{4.6}$$

Аналогічним чином, для формату 4:1:1 отримуємо:

$$V(t)^{(Y)} = H_Y W_Y \mu\beta\varepsilon \tag{4.7}$$

Відтак, спочатку потрібно обчислити значення величини $\beta$. Для нашого випадку попередньо необхідно розрахувати кількість B-кадрів, які входять у зазначений часовий проміжок.

Нехай $\alpha$ - загальна кількість кадрів у групі. При цьому в умовах, що кодек щосекунди формує $\eta$ кадрів, секундний часовий відрізок включатиме у себе $\lambda$ цілих груп кадрів, тобто [12]:

$$\lambda = \mathrm{div}(\frac{\eta}{\alpha}). \tag{4.8}$$

Водночас, для неповної групи обсяг $\alpha'$ кадрів може бути розраховано згідно з наступним виразом:

$$\alpha' = \eta - \mathrm{mod}(\frac{\eta}{\alpha}). \tag{4.9}$$

У випадку, коли розглядається група мінімальної довжини (тобто, $\alpha = 8$), тоді в умовах, коли частота слідування кадрів рівна $\eta = 30$, отримуємо $\lambda = \mathrm{div}(\frac{30}{8}) = 3$, а $\alpha' = 30 - \mathrm{mod}(\frac{30}{8}) = 6$.

Разом з тим, для групи мінімальної довжини обсяг кадрів B-типу дорівнює 5. Отже, у цих умовах 3 повні групи міститимуть у собі $\alpha_B = 3 \times 5 = 15$ B-кадрів.

Далі, виконавши аналіз рисунку 2.1 можемо бачити, що коли $\alpha' = 6$, тоді $\alpha'_B = 4$. Отже, загальну кількість $\beta$ кадрів B-типу, які входять у секундний відрізок часу, може бути визначено, як:

$$\beta = \alpha_B + \alpha'_B. \tag{4.10}$$

Таким чином, у даному разі, керуючись виразом (4.10), маємо $\beta = 15 + 4 = 19$.

Тоді, керуючись виразом (4.5), отримуємо $V(t)^{(YCrCb)}_{4:4:4} = (1920 \times 1080 \times 3) \times 1 \times 19 \times 0{,}1 = 11{,}8$ Мбіт (1,48 МБ).

У свою чергу, для формату 4:1:1, згідно з виразом (4.6), обсяг біт, що можуть надсилатися протягом секундного інтервалу, дорівнює

$$V(t)_{4:1:1}^{(YCrCb)} = (1920 \times 1080 + \frac{1920 \times 1080}{4} + \frac{1920 \times 1080}{4}) \times 1 \times 19 \times 0{,}1 \approx 5{,}9$$ Мбіт,

або 0,74 МБ.

При цьому, для випадку, коли дані вбудовуються виключно у LSB яскравісного простору, відповідно до формули (4.7) маємо $V(t)^{(Y)} = 1920 \times 1080 \times 1 \times 19 \times 0{,}1 = 3{,}93$ Мбіт (0,49 МБ).

Тепер обчислимо теоретично доступну ємність мультиконтейнерної структури за умови застосування адаптивних алгоритмів LSB, тобто, для випадку найвищої захищеності. Як і для статичного контейнеру, тут розрахунок виконується з огляду на те, що умовна ємність одного контейнеру (кадр B-типу) за умови використання адаптивних алгоритмів є не більшою, ніж 10% доступного простору вбудовування.

Виходячи з зазначеного міркування, для формату 4:4:4 захищений об'єм даних дорівнює $\hat{V}(t)_{4:4:4}^{(YCrCb)} = 0{,}1\, V(t)_{4:4:4}^{(YCrCb)} = 1{,}18$ Мбіт (0,15 МБ).

Тоді для формату 4:1:1 - $\hat{V}(t)_{4:1:1}^{(YCrCb)} = 0{,}1\, V(t)_{4:1:1}^{(YCrCb)} = 0{,}59$ Мбіт, чи 0,074 МБ.

У свою чергу, для випадку використання виключно яскравісного простору, отримуємо $\hat{V}(t)^{(Y)} = 0{,}1\, V(t)^{(Y)} = 0{,}393$ Мбіт (0,049 МБ).

Отримані результати оцінки потенційно можливої ємності стеганографічного каналу на базі класичного та адаптивних алгоритмів LSB з використанням у якості мультиконтейнерної структури множини B-кадрів потоку 1920x1080 для різних режимів реалізації показано табл. 4.1.

Таблиця 4.1 - Результати оцінки потенційно можливої ємності стеганографічного каналу для різних варіантів реалізації

| | Окремий контейнер, Мбіт | | | Мультиконтейєрна структура, Мбіт/с | | |
|---|---|---|---|---|---|---|
| Формат | 4:4:4 | 4:1:1 | Канал Y | 4:4:4 | 4:1:1 | Канал Y |
| Класична реалізація LSB | 0,633 | 0,31 | 0,207 | 11,8 | 5,9 | 3,93 |
| Адаптивні алгоритми | 0,0633 | 0,031 | 0,0207 | 1,18 | 0,59 | 0,393 |

Як показує аналіз табл. 4.1, максимальна ємність прихованого каналу обміну даними може становити у нашому випадку 11,8 Мбіт/с. Це відповідає використанню усього простору Y, а також Cr і Cb у форматі 4:4:4 та застосовуючи класичний варіант LSB (повне заповнення).

Разом з тим, у даному режимі, по-перше, забезпечується найнижчий рівень захищеності вбудованих даних, оскільки алгоритм є нестійким до методів візуального аналізу. По-друге, використання формату 4:4:4 є невиправданим за показником якість/інтенсивність для випадку відеоряду, що надсилається мережею. У підсумку, попри високу ємність, зазначені чинники не дозволяють розглядати зазначений режим як такий, що є прийнятним для створення прихованого відеоканалу.

У свою чергу, використання адаптивних LSB-алгоритмів відносно контейнерів колірного формату 4:1:1, або, навіть, виключно каналу Y, дозволяє забезпечити формування прихованого каналу, ємності якого достатньо для передавання потокового відео. Про це свідчить дослідження номіналів інтенсивностей відео (зі звуковим рядом), розміщеного на відео сервері YouTube. Для дослідження було використано плагін Video Download Helper [22], що входить до набору розширень Mozilla Firefox.

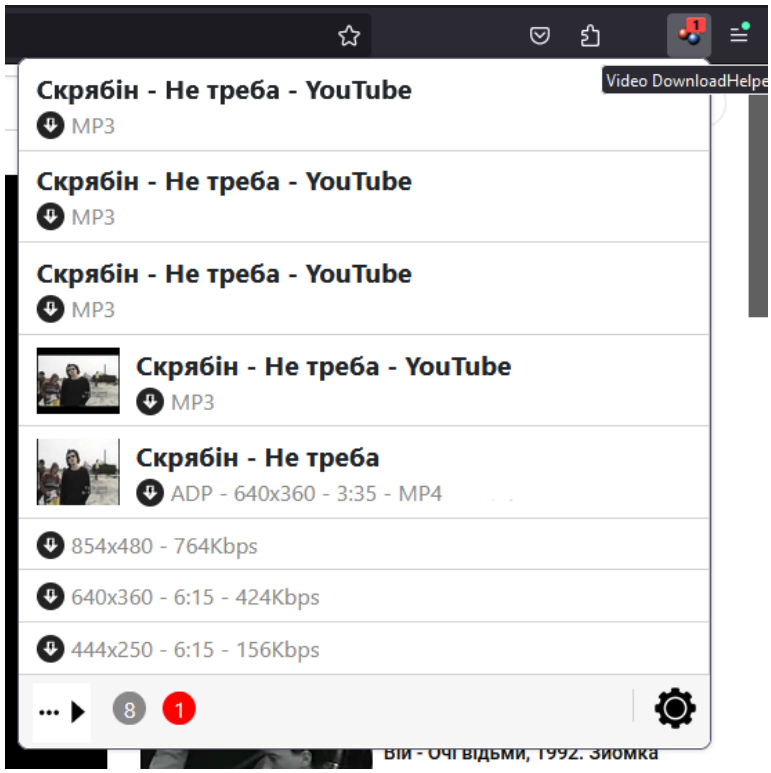



Рисунок 4.1 – Приклади номіналів інтенсивностей відео, завантажених на YouTube

Таким чином, як можна бачити з аналізу табл.4.1 та рис. 4.1, використання адаптивних LSB алгоритмів у випадку, коли контейнером є відео FullHD, дозволяє створити приховану потокову передачу відео з роздільною здатністю до 640x360, забезпечуючи при цьому захищеність прихованих даних.

# ВИСНОВКИ

У рамках вирішення завдань, наведених у технічному завданні, було виконано:

- аналіз принципів побудови систем прихованої інформаційної взаємодії;

- аналіз основних модулів у складі системи прихованої інформаційної взаємодії;

- дослідження суті механізмів вбудовування даних; - розгляд принципів перетворення даних у рамках базису MPEG-обробки;

- дослідження можливості побудови прихованого каналу, що забезпечує передачу відеоряду потокового типу, а також приблизна оцінка рівня інтенсивності прихованого відеопотоку.

Зокрема, у ході дослідження було виявлено, що, виходячи з ключових вимог до контейнерів системи прихованої передачі інформації, в умовах необхідності забезпечити доставку відеоданих, найбільш високим потенціалом має варіант реалізації системи на основі відеоряду в ролі контейнерного матеріалу.

Щоб оцінити потенційно доступний обсяг відео потоку у ролі мультиконтейнерної структури, попередньо виконано аналіз базових механізмів MPEG.

Аналіз проводився для умов, коли як алгоритмом вбудовування даних приховуваного повідомлення розглядався класичний LSB, а також його гіпотетична адаптивна версія.

При цьому, розрахунок проводився для несучого відеопотоку середньої динаміки зміни кадрів.

У результаті такого аналізу було виявлено, що:

- у рамках відеоряду, з точки зору можливості забезпечення найвищої захищеності вбудовуваного прихованого контенту, у ролі контейнерів найбільш доцільно використовувати кадри B-типу;

- для випадку, коли контейнерною структурою розглядається відеоряд з роздільною здатністю кадру на рівні FullHD (1920x1080) за умови стандартної частоти надходження кадрів, може бути забезпечена можливість потокової передачі відеоряду SD формату 640x360.

У той же час, для того, щоб гарантувати можливість прихованої трансляції відео, в ролі несучого потоку доцільно розглядати відеоряд середньої або високої динаміки.

Таким чином, усі пункти технічного завдання виконані повною мірою.

# ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Microsoft security report [Електронний ресурс] – Режим доступу: https://microsoft.com/securityinsights.

2. Antivirus and Cybersecurity Statistics & Facts 2021 [Електронний ресурс] – Режим доступу: https://wethegeek.com/antivirus-statistics-facts/

3. Wrightson T. Advanced Persistent Threat Hacking: The Art and Science of Hacking Any Organization. – McGraw-Hill, - 2014. – 464 p. ISBN: 9780071828376

4. Stood, A. Targeted Cyber Attacks. — Elsevier Inc.. — 2014. — ISBN 978-0-12-800604-7.

5. Шелухін О.И., Канаєв С.Д. Стеганографія. Алгоритми і програмна реалізація. Гаряча лінія – Телеком, науково-технічне видавництво, 2017, 592 с.

6. Шаньгін В.Ф. Захист інформації в розподілених корпоративних мережах і системах [Текст]: підручник / В.Ф. Шаньгин, А.В. Соколов. – М.: ДМК Пресс, 2002. – 656 с.

7. Стеганография в современных кибератаках | Securelist [Електронний ресурс] – Режим доступу: https://securelist.ru/steganography-in-contemporary-cyberattacks/79090.

8. Fridrich Y. Steganography in Digital Media: Principles, Algorithms and Applicaticks. Cambridge Press, 2010. 462.

9. Грибунін В. Г., Оков И. Н., Турінцев И. В. Цифрова стеганографія. СОЛОН-Прес, 2016, - 315 с.

10. Цифровая стеганографія: Програми та інші способы реалізації [Електронний ресурс] – Режим доступу: http://www.spy-soft.net/cifrovaya-steganografiya-sposoby-realizacii/

11. VNI Forecast Highlights Tool [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/m/en_us/solutions/service-provider/vni-forecast-highlights.html

12. Річардсон Ян. H.264 and MPEG-4 Video Compression: Video Coding for Next-Generation Multimedia / Ян Річардсон. – 2005. – 368 с.

13. Селомон Д. Стиснення даних, зображень та звуку / Д. Селомон. – Техносфера, 2004. – 368 с.

14. Р. Гонсалес, Р. Вудс. Цифрова обробка зображень —Техносфера, 2005 – 1007 с.

15. Shi, Yun Q. Image and video compression for multimedia engineering: fundamentals, algorithms, and standards / Yun Q Shi, Huifang Sun.

16. Алексєєв, А.П. Стеганографічні та криптографічні методи захисту інформації : навч. посібн. з дисципліни "Інформатика" / В.В. Орлов, А.П. Алексєєв. 2010 .— 289 с.

17. Шаньгін В.Ф. Інформаційна безпека та захист інформації. ДМК-Прес., 2017, 702 с.

18. Рябко Б.Я. Основи сучасної криптографії та стеганографії: [монографія] / А.Н. Фіонов, Б.Я. Рябко. — Гаряча лінія – Телеком, 2010 .— 233 с.

19. Конахович Г. Ф., Пузиренко А. Ю. Комп’ютерна стеганографія. Теорія і практика. - К.: МК-Пресс, 2006. - 288 с

20. Биков С. Ф. Алгоритм стиснення JPEG з позиції комп’ютерної стеганографії. Захист інформації. Конфідент.: 2000, № 3.

21. Dumitrescu, S., W. Xiaolin and Z. Wang, 2003. Detection of LSB steganography via sample pair analysis. In: LNCS, Vol. 2578, Springer-Verlag, New York, pp: 355-372.

22. Download Helper – Video download browser extension [Електронний ресурс] Режим доступу: http://www.downloadhelper.net