

## ДОДАТОК А СЛАЙДИ ПРЕЗЕНТАЦІЇ

Харківський національний університет радіоелектроніки  
Кафедра ІМІ

Магістерська кваліфікаційна робота  
на тему

**Дослідження криптокомпресійних методів обробки  
інтерактивного відео на базі поліадичного коду з нефіксованими  
вагами**

Виконав: Ольховський В.І.  
Керівник: ст.викл. Твердохліб В.В.

Харків - 2021

2

## МЕТА РОБОТИ

Дослідження методів та умов обробки інтерактивної відеоінформації, які забезпечують скорочення часу побудови шифрограм

### ЗАВДАННЯ, ЯКІ НЕОБХІДНО ВИРІШИТИ

1. Розглянути вимоги до процесу обробки відеоінформації
2. Виконати вибір та обґрунтування підходу, що дозволяє мінімізувати кількість обчислювальних операцій у ході шифрування ключових кадрів
3. Дослідити поширені алгоритми шифрування даних
4. Дослідити можливості застосування поліадичний кодів нефіксованої ваги у базисі *jpeg* для зменшення обчислювального навантаження у ході формування шифрограм

Проблематика процесу обробки відеоінформації

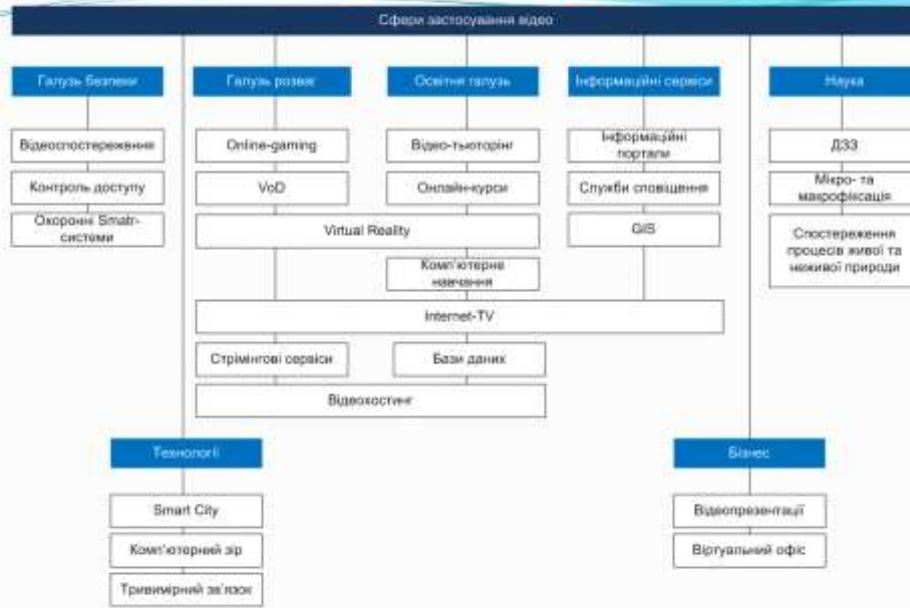


Рисунок 1 – Сфери застосування відео

Проблематика процесу обробки відеоінформації



Рисунок 2 – Переваги та недоліки підходів до забезпечення захисту відеоінформації з обмеженням доступом

Загальна затримка доставки пакетів відео:

$$t = t_{зм} + t_{екс} + t_{ш} + t_{об} + t_{ст} \leq t_{ст} \quad (1)$$

- де  $t_{зм}$  - час безпосередньо формування відеоінформації джерелом;
- $t_{екс}$  - час, який витрачається на кодування оформованих відеоданих;
- $t_{ш}$  - час шифрування відео;
- $t_{об}$  - час загальної обробки, куди входить пакетування кодованих даних, переміщення їх до вихідного буферу тощо;
- $t_{ст}$  - час, який займає передавання відео мережею;
- $t_{ст}$  - стандартизована величина затримки, що є допустимою за QoS.

Час формування відеоінформації для потокового відео, яке є попередньо обробленим:

$$t_{зм} = t_{екс} = t_{ш} = 0 \quad (2)$$

Наближений вираз для сумарної затримки відео потокового типу:

$$t_{st}(str) = t_{об} + t_{ст} \quad (3)$$

Взаємозв'язок між існуючими вимогами до затримки для інтерактивного та потокового відео:

$$t_{st}(inf) < t_{st}(str) \quad (4)$$

Умови ефективного обробки інтерактивної відеоінформації з використанням шифрування відповідно до вимог QoS:

$$t_{ш} \rightarrow \min \quad (5)$$

## Проблематика процесу обробки відеоінформації

5

Поточний обсяг біт для потоку кодованих кадрів як структури, неоднорідної у часі:

$$\eta(t) = f(Q(t)_I; Q(t)_{type}), \quad (6)$$

де  $Q(t)_I$  - особливості вмісту Q-го кадру відеопотоку, що обробляється у поточний час  $t$ ;

$Q(t)_{type}$  - фактор належності Q-го кадру відеопотоку до одного з типів, прийнятих у MPEG.

Кількість біт, що містить група кадрів:

$$N(G_i) = \eta(Q_i) + \sum_{k=1}^K \eta(Q_p^{(k)}) + \sum_{l=1}^L \eta(Q_B^{(l)}), \quad (7)$$

де  $\eta(Q_i)$ ,  $\eta(Q_p^{(k)})$  та  $\eta(Q_B^{(l)})$  - кількість біт, що вносяться кадрами I, P та B типу відповідно;

K та L - кількість P та B-кадрів у групі.

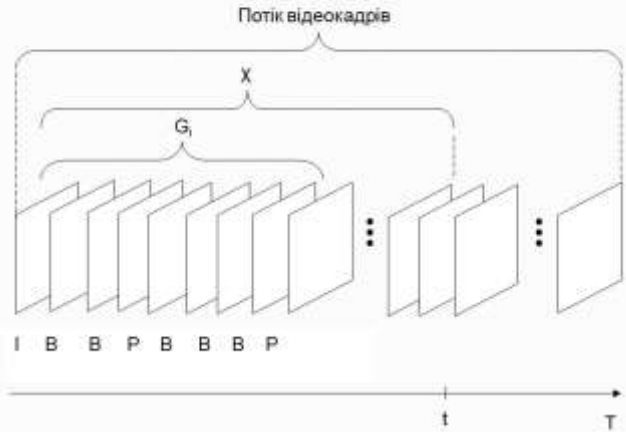


Рисунок 3 – Група кадрів у структурі відеопотоку

## Проблематика процесу обробки відеоінформації

6



Рисунок 4 – Схематичне зображення типового взаємозв'язку між кадрами у групі

Шляхи мінімізації кількості обчислювальних операцій у ході шифрування ключових кадрів



Таблиця 1 – Потенційно можливий об'єм даних, які підлягають шифруванню, для вилучу відеокадрів форматів 2К та 4К за умови, що  $\chi=30$

Роздільна здатність	Окремий ключовий кадр	G = 8	G = 32
2К	0,25515 Мб	0,76545 Мб	0,25515 Мб
4К	1,548288 Мб	4,644864 Мб	1,548288 Мб

Рисунок 5 – Способи організації технологічного етапу шифрування даних на базі JPEG-платформи

Дослідження поширених алгоритмів шифрування

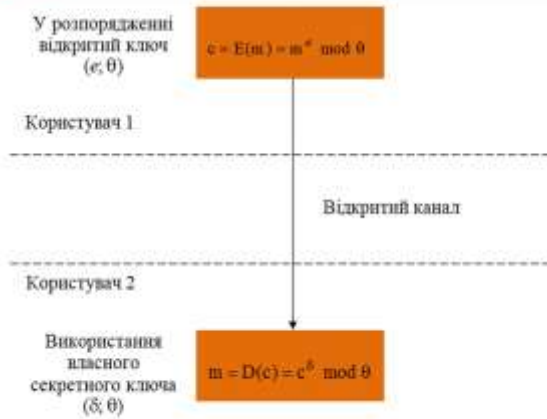


Рисунок 6 – Загальна схема формування шифрограми повідомлення та його дешифрування з використанням алгоритму RSA

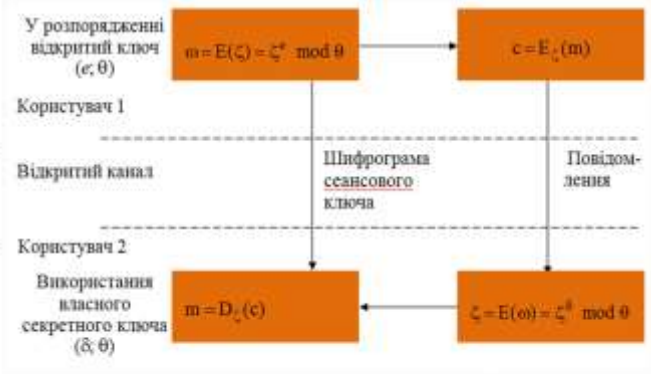


Рисунок 7 – Схема формування шифрограми повідомлення та його дешифрування з використанням алгоритму RSA для умов застосування сеансового ключа

## Дослідження поширених алгоритмів шифрування

9

Принцип використання залежності між окремими складниками повідомлення для зменшення ймовірності розшифрування тексту:

$$b := f(b; a; k), \quad (8)$$

де  $a$  – передуючий елемент повідомлення;  
 $b$  – наступний елемент повідомлення;  
 $k$  – елемент ключа шифрування.

Наприклад, елементи повідомлення може бути змінено на базі виразу  $b := (b + a) \% \theta$ .



Рисунок 8 – Ключові вимоги до процесу вибору простих чисел для розрахунку модулю RSA

## Дослідження поширених алгоритмів шифрування

10

Вимога до процесу підбору величин  $\alpha$  і  $\beta$ :

$$t_{gen} \rightarrow \min, \quad (9)$$

де  $t_{gen}$  – час, протягом якого генеруються величини  $\alpha$  і  $\beta$

Принцип вибору розмірності секретної експоненти  $\delta$ :

$$\begin{cases} \delta \uparrow \rightarrow S \uparrow \& \uparrow t_d; \\ \delta \downarrow \rightarrow S \downarrow \& \downarrow t_d. \end{cases} \quad (10)$$

де  $S$  – рівень захищеності шифрограми;  
 $t_d$  – час дешифрування.

Умова, за якої зловмисник може відновити приватний ключ використовуючи атаку Вінера:

$$\delta < \sqrt[4]{\theta}. \quad (11)$$

Вимога щодо черговості формування величин, необхідних для реалізації алгоритму RSA:

- модуль  $\theta$ , використовуючи значення  $\alpha$  і  $\beta$ ;
- публічна експонента  $e$ ;
- секретна експонента  $\delta$ .

Недоліки алгоритму RSA та його реалізації:

- які стосуються процедури генерування простих чисел для обчислення модулю RSA;
- недоліки вибору розмірності секретної експоненти;
- зумовлені величиною публічної експоненти

Таблиця 2 – Кількість раундів виконання алгоритму AES залежно від розміру використаного ключа

Довжина ключа, біт	$N_{\text{rnd}}$
128	10
192	12
256	14

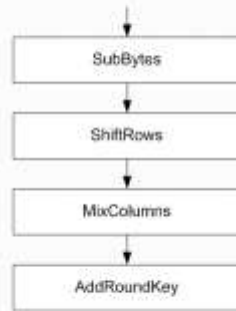


Рисунок 9 – Загальна схема виконання технологічних етапів у складі алгоритму AES

Етап SubBytes

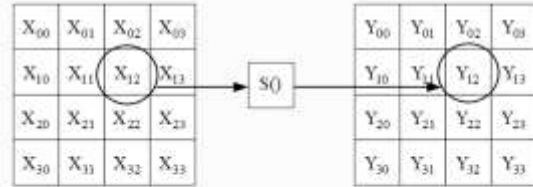


Рисунок 10 – Принцип табличної заміни масиву байт вихідного блоку

Кроки побудови таблиці S-бок (операнд S()):

- обчислення зворотного числа у полі Галуа;
- перетворення кожного байту, що формує S-бок, відповідно до виразу:

$$b'_i = b_i \oplus b_{i+4 \bmod 8} \oplus b_{i+5 \bmod 8} \oplus b_{i+6 \bmod 8} \oplus b_{i+7 \bmod 8} \oplus c_i, \quad 0 < i < 8, \quad (12)$$

де  $b_i$  -  $i$ -й біт байту  $b$ ;  $c_i$  -  $i$ -й біт, що належить константі  $c = 63_{16} = 99_{10} = 01100011_2$ .

Етап ShiftRows



Рисунок 11 – Схематичне зображення виконання процесу ShiftRows

Етап MixColumns

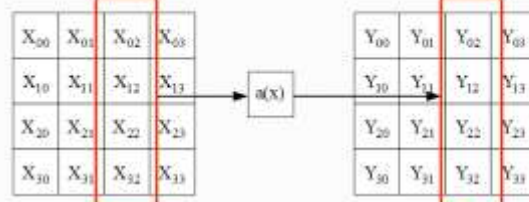


Рисунок 12 – Принцип виконання технологічного процесу MixColumns

Поліном  $a(x)$  на який перемножуються за модулем  $(x^4 + 1)$  усі стовпці масиву на етапі MixColumns:

$$a(x) = 3x^3 + x^2 + x + 2. \quad (13)$$

## Етап AddRoundKey

Накладення секретного ключа на масив байт стовпця  $B_i$ :

$$B_i^r = B_i \oplus W_{t+r,i} \quad (14)$$

де  $B_i$  –  $i$ -й стовпець масиву;

$B_i^r$  – шифрований стовпець масиву;

$W_{t+r,i}$  – кодове слово-ключ;

$t$  – індекс поточного раунду виконання шифрування

Особливості алгоритму AES:

- для шифрування даних рівня SECRET може бути використано ключ довжиною 128 біт;
- дані рівня TOP SECRET необхідно шифрувати ключами довжиною 192 та 256 біт.

Підходи щодо зламу AES-шифрів:

- XSL-атаки;
- атаки за сторонніми параметрами (атаки за часом)

## Застосування поліадичний кодів нефіксованої ваги у базисі жред для зменшення обчислювального навантаження у ході формування шифрограм

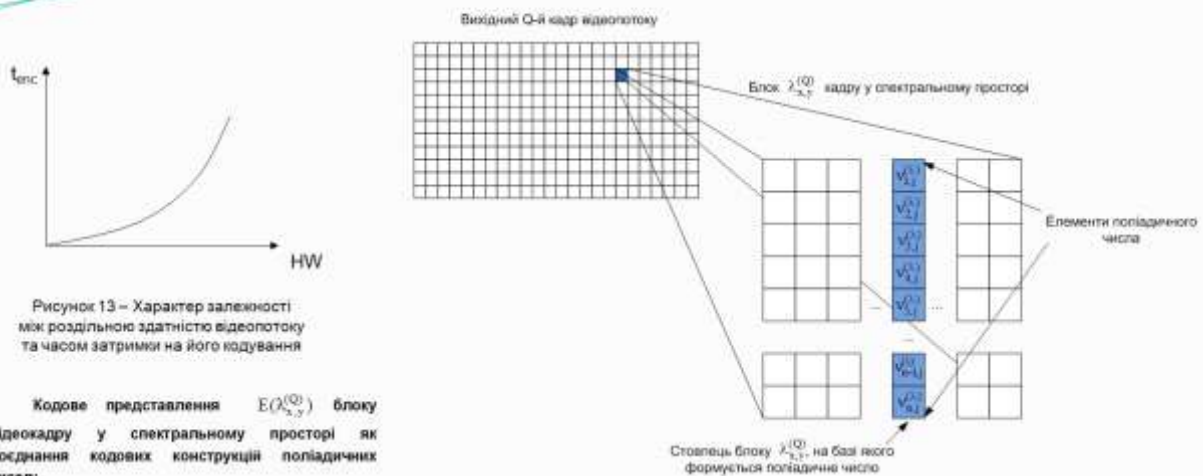


Рисунок 14 – Локалізація елементів поліадичних чисел за стовпцями блоку для побудови його кодового опису

## Застосування поліадичних кодів нефіксованої ваги у базисі j-ред для зменшення обчислювального навантаження у ході формування шифрограм

15

Обчислення основ рядків:

$$\vartheta_i = \max(v_{ij}^{(k)}) + 1, \quad (16)$$

де  $v_{ij}^{(k)}$  - елемент поліадичного числа

Розрахунок вагових коефіцієнтів елементів поліадичних чисел:

$$\Psi_j = \prod_{k=j+1}^n \vartheta_{ik}, \quad (17)$$

Формування поліадичних чисел  $\Theta_i$ :

$$\Theta_i = \sum_{j=1}^n [v_{ij}^{(k)} \times \Psi_j]. \quad (18)$$

Умова, що доводить доцільність шифрування саме системи основ, а не безпосередньо множини поліадичних чисел:

$$\vartheta_i < \Theta_i, \quad (19)$$

Система основ (службова інформація)

Масив поліадичних чисел

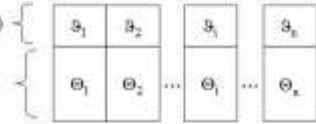


Рисунок 15 – Структура кодограми блоку кадру

## Застосування поліадичних кодів нефіксованої ваги у базисі j-ред для зменшення обчислювального навантаження у ході формування шифрограм

16

Таблиця 3 – Зведені відомості щодо кількості даних, які необхідно шифрувати для відео потоків при використанні ймовірно-статистичного кодування та поліадичних кодів з нефіксованими вагами.

Роздільна здатність	Ймовірно-статистичне кодування			Поліадичний код з нефіксованими вагами		
	Окремий ключовий кадр	G = 8	G = 32	Окремий ключовий кадр	G = 8	G = 32
2К	0,25515 Мб	0,76545 Мб	0,25515 Мб	0,0324 Мб	0,0972 Мб	0,0324 Мб
4К	1,548288 Мб	4,644864 Мб	1,548288 Мб	0,196608 Мб	0,589824 Мб	0,196608 Мб

## ВИСНОВКИ

17

1. Виконано дослідження підходів щодо забезпечення ефективної побудови шифротрам відеоінформаційних потоків реального часу.
2. Обґрунтовано, що забезпечення ефективного шифрування інтерактивного відеоконтенту вимагає мінімізації часу, що витрачається на шифрування; зменшення часу, який займає процедура кодування.
3. Показано, що в існуючих умовах більш надійним є надсилання одеракувачам кодованих відеоданих, замість їх трансляції захищеним каналом у відкритому вигляді.
4. У рамках дослідження підходів до подальшого скорочення часу шифрування виконано оцінку обсягу даних, які підлягають шифруванню, в умовах, коли кодування ключових кадрів виконується за загальними принципами JPEG, характерними для MPEG-платформи. При цьому виявлено, що найбільший обсяг даних, що мають шифруватися щосекунди, відповідає випадку, коли розмірність групи у рамках відеопотоку є мінімальною та дорівнює 8. У свою чергу, обсяг даних, які необхідно шифрувати за секунду за умов групи максимального розміру (32 кадри) є найменшим, та відповідає об'єму одного ключового кадру.
5. Виявлено, що для випадку потоку відео 4K та групи мінімального розміру обсяг шифрованих даних є критичним. Отже, за цих умов необхідно використовувати більш швидкий алгоритм шифрування, розглянути підхід, у рамках з відеокадру може бути виокремлено найбільш критичні складові, шифрування яких, по-перше дозволить повністю закрити кадр, по-друге – займе значно менше часу на обробку.
6. Досліджено підхід, у рамках якого здійснюється заміна класичного алгоритму ймовірно-статистичного кодування зі складу JPEG поліадичним кодом з нефіксованими вагами. Такий підхід передбачає формування на базі вихідної кількості компонент блоку кадру після його квантизації у спектральному просторі ряду поліадичних чисел, кількість яких завжди є фіксованою та дорівнює кількості стовпців (рядків) блоку. Тобто, перевагами такого підходу є детермінована кількість математичних операцій у ході кодування; апріорі відома і постійна кількість підсумкових поліадичних чисел, що утворюються за результатами кодування; той факт, що кількість сформованих поліадичних чисел завжди є меншою  $p$  разів по відношенню з кількістю  $px$  компонент після процедури квантування. Отже, відповідно до даного підходу шифруванню підлягає службова інформація – система основ, яка являє собою  $p$  десяткових чисел, які використовуються для відновлення кодограми на прийомному боці.
7. Показано, що за даних умов для найгіршого випадку кількість біт, які необхідно шифрувати у складі ключового кадру, майже у 7,9 разів є меншою, ніж для випадку, коли використовується ймовірно-статистичний підхід на етапі кодування без втрат у JPEG.
8. У ході дослідження алгоритмів шифрування даних виявлено, що криптографічна система AES є доцільною для застосування як базовий інструмент шифрування відео.

ДЯКУЮ ЗА УВАГУ!

ДОДАТОК Б  
ПУБЛІКАЦІЯ

**SCI-CONF.COM.UA**

**MODERN SCIENCE:  
INNOVATIONS AND  
PROSPECTS**



**ABSTRACTS OF II INTERNATIONAL  
SCIENTIFIC AND PRACTICAL CONFERENCE  
NOVEMBER 7-9, 2021**

**STOCKHOLM  
2021**

51. *Полянський О. С., Д'яконов В. І., Д'яконов О. В., Насальський В. А., Пиріжок В. С.* 286  
 ПЕРЕРОБКА ВІДХОДІВ МЕБЛЕВИХ ВИРОБНИЦТВ В  
 ГЕНЕРАТОРНИЙ ГАЗ ГАЗОГЕНЕРАТОРНИХ ДВИГУНІВ З  
 ВИКОРИСТАННЯ НВЧ-ТЕХНОЛОГІЙ.
52. *Скрыпник В. С., Журавлев Д. Ю., Андрейчиков Е. Ю., Болонный В. Т.* 292  
 ЭФФЕКТИВНОСТЬ ТЕПЛООБМЕНА В ПАРАХ ТРЕНИЯ ТОРМОЗОВ.
53. *Сорокіна А. П., Бабич М. І.* 302  
 ДОСЛІДЖЕННЯ МЕТОДИКИ ПРОГНОЗУВАННЯ СПОРТИВНИХ  
 РЕЗУЛЬТАТІВ СПОРТСМЕНІВ ДЛЯ ФОРМУВАННЯ  
 РАЦІОНАЛЬНОГО СКЛАДУ ЗБІРНОЇ.
54. *Стефанович І. С., Стефанович П. І., Прокопенко І. О.* 306  
 ЯДЕРНИЙ ВИБУХ ТА ЙОГО ВРАЖАЮЧІ ФАКТОРИ.
55. *Твердохліб В. В., Харченко Н. А., Калініченко В. М., Галушка С. В., Дяченко Д. А.* 313  
 ШЛЯХИ ЗБІЛЬШЕННЯ ПРОДУКТИВНОСТІ ІСНУЮЧИХ МЕТОДІВ  
 КОДУВАННЯ ВІДЕОІНФОРМАЦІЇ.
56. *Твердохліб В. В., Юрченко В. Р., Ольховський В. І., Дяченко Д. А.* 317  
 АНАЛІЗ АЛГОРИТМІВ БАЛАНСУВАННЯ БІТОВОЇ ШВИДКОСТІ  
 ВІДЕО ТРАФІКУ РЕАЛЬНОГО ЧАСУ.
57. *Фіалко Н. М., Дінжос Р. В., Прокопов В. Г., Мерапова Н. О.* 323  
 ЗАЛЕЖНІСТЬ ГУСТИНИ НАНОКОМПОЗИТІВ ВІД ВЕЛИЧИНИ  
 ПЕРЕГРІВУ РОЗПЛАВУ ПОЛІМЕРУ.
58. *Харченко Н. А., Бойчук М. І., Дяченко Д. А.* 328  
 ПІДХІД ДО ЗБІЛЬШЕННЯ ПРОДУКТИВНОСТІ ПРОЦЕСІВ ОБРОБКИ  
 МУЛЬТИМЕДІЙНОГО ТРАФІКУ.
59. *Чупайленко О. А., Ломова К. В., Журавель Н. В.* 331  
 ПРОПУСКНА ЗДАТНІСТЬ АВТОМОБІЛЬНИХ МІЖНАРОДНИХ  
 ТРАНСПОРТНИХ КОРИДОРІВ.
60. *Штрибець В. В., Трофименко А. О., Бойко С. О., Ткаченко В. В.* 335  
 АНАЛІЗ МЕТОДІВ ВИЗНАЧЕННЯ ДЕФЕКТІВ ПІДШИПНИКІВ  
 СУДНОВИХ ВАЛОПРОВОДІВ.
- PHYSICAL AND MATHEMATICAL SCIENCES**
61. *Піпа К. Е., Lystopadova V. V.* 340  
 UNSOLVABLE MATHEMATICAL PROBLEMS AND THEIR IMPACT  
 ON STUDENTS.
- ARCHITECTURE**
62. *Тіхонова О. А.* 343  
 АСПЕКТИ GREEN BIM-МОДЕЛЮВАННЯ В АРХІТЕКТУРІ.
63. *Фостащенко О. М., Архіпова К. К., Фостащенко Д. О., Трушина В. С., Захарова С. О.* 348  
 ПРОБЛЕМНІ АСПЕКТИ РЕНОВАЦІЇ ПАРКІВ МІСТА ЗАПОРІЖЖЯ.

## АНАЛІЗ АЛГОРИТМІВ БАЛАНСУВАННЯ БІТОВОЇ ШВИДКОСТІ ВІДЕО ТРАФІКУ РЕАЛЬНОГО ЧАСУ

**Твердохліб Віталій Вікторович**

к.т.н.

**Юрченко Владислав Русланович**

студент

**Ольховський Володимир Іванович**

студент

**Дяченко Денис Андрійович**

студент

Харківський національний університет радіоелектроніки  
м. Харків, Україна

**Вступ.** Забезпечення якості надання відеоінформаційних мережевих послуг сьогодні є одним з найбільш актуальних завдань. Це зумовлюється як постійним ростом затребуваності даного класу послуг у суспільстві, так і складністю підтримки параметрів відеотрафіку на належному рівні. Це зумовлюється як жорсткими вимогами QoS щодо показників якості відновленого відео (найбільшою мірою – інтерактивного типу), так і нестабільністю пропускної здатності мережевих каналів. Тому на рівні джерела відеоданих необхідно побудувати процес кодування таким чином, щоб забезпечити динамічну зміну біткової швидкості стисненого потоку відповідно до змін поточного рівня пропускної здатності.

**Мета роботи.** Аналіз існуючих алгоритмів та технологій балансування біткової швидкості відео щодо пропускної здатності мережі.

**Матеріали і методи.** Аналізуються ключові методи та алгоритми, задіяні у процесі управління бітковою швидкістю потоку кодованих кадрів. Їхні виявлені недоліки обґрунтовуються базі системного підходу, базуючись на використанні теоретичного інструментарію аналізу складних систем. Висновки щодо проаналізованих методів та алгоритмів робляться з огляду на положення теорії інформації та кодування.

У загальному випадку зараз можна виділити 2 напрямки балансування бітової швидкості відео у мережі:

1. На рівні мережеских вузлів. Даний підхід ґрунтується на використанні «розумних черг» за пріоритетністю пакетів, резервуванні фізичних каналів та використанні протоколів маршрутизації. Завданням даного підходу є зменшення пульсуючого характеру відеотрафіку на ділянці мережі шляхом його перерозподілу, що забезпечується за умови, коли навантаження на мережеві вузли не перевищує у середньому 40%. Недоліки даного підходу такі:

- сумарне навантаження мережі при цьому не змінюється;
- підхід є неефективним при зростанні навантаження на мережеві вузли;
- в умовах надходження на мережевий вузол великої кількості пакетів, що належать різномірним сервісам критичного та інтерактивного типів за класифікацією QoS зростає ймовірність втрат деякої частини пакетів відеоданих.

2. На рівні джерела відеоінформації. Передбачається, що тут бітова швидкість  $V(t)$  пов'язана деякою функціональною залежністю  $V(t) = f(B(t))$  з пропускнуою здатністю  $B(t)$  мережі. При цьому, функціонал  $f$  описує механізм управління рівнем  $V(t)$  бітової швидкості з урахуванням  $B(t)$ .

На цьому принципі, зокрема, базується алгоритм SRC (scalable gate control), що входить до складу MPEG4 Part10. Алгоритм реалізовано на рівні кадру (грубий алгоритм), а також на рівні макроблоку (точний алгоритм). У першому випадку бітова швидкість  $V(t)$  джерела визначається як:

$$V(t) = \frac{\delta_1 \Lambda}{\ell} + \frac{\delta_2 \Lambda}{\ell^2}, \quad (1)$$

де  $\delta_1$  і  $\delta_2$  - відповідно, параметри моделі;

$\ell$  - величина кроку квантування;

$\Lambda$  - параметр складності кадру, (величина середньої абсолютної різниці залишкового кадру після компенсації руху).

Даний реліз алгоритму SRC застосовується на етапі обробки, наступному після етапу компенсації руху і передуючому обробці  $i$ -го кадру. На відміну від

грубого механізму управління інтенсивністю, точний механізм (розширення алгоритму SRC) орієнтований на роботу з макроблоками. Отже, у процесі обробки відеопотоку проводиться зміна величини  $\ell$  на рівні макроблоків, чим забезпечується більш точний контроль інтенсивності відеоданих

При цьому, у ході роботи алгоритму виконується визначення необхідного обсягу біт  $R_{mb}$  для кодування макроблоку, як показано наступним виразом:

$$V(t)_{mb} = HW(K \frac{\chi_i^2}{q_i} + C), \quad (2)$$

де  $HW$  - кількість пікселів у межах поточного макроблоку;

$\chi_i$  - величина відмінності значень хроматичності і яскравості залишкового макроблоку, що виражається через середньоквадратичне відхилення даних параметрів;

$\ell_i$  - величина кроку квантування;

$K$  і  $C$  - постійні параметри моделі.

У ході балансування бітової швидкості величина  $\ell_i$  знаходиться за величинами  $K$ ,  $C$ ,  $R_{mb}$  і  $\chi_i$  та беручи до уваги вагу  $q_i$  поточного макроблоку. При цьому, параметр  $q_i$  позначає рівень важливості, поточного макроблоку для суб'єктивного сприйняття відеокадру. Низькі значення  $q_i$  призначаються макроблокам, що не вносять суттєвого вкладу при візуалізації. Для них, у свою чергу, встановлюється величина кроку  $\ell_i$ , що сприяє їх квантування більш значно, ніж інших макроблоків.

Також значення величини  $q_i$  обирається з урахуванням мінімізації змін кроку квантування на випадок низьких бітових швидкостей. Це зумовлено тим, що у разі кожної зміни  $\ell_i$  здійснюється зростання обсягу службових даних у межах макроблоку на 5 біт. Тобто, на випадок незначних величин бітової швидкості ріст обсягу службової інформації може бути критичним, відтак - необхідно скоротити кількість змін  $\ell_i$ .

Разом з тим, дане обмеження відносно кількості змін значення кроку

квантування не поширюється на випадки обробки відеоданих з високою інтенсивністю. Тобто, при значній бітовій швидкості допускається часта зміна параметра  $\ell_i$ . Таким чином, за умови малого обсягу вихідного буфера кодера даний підхід до управління інтенсивністю дозволяє забезпечити:

- візуальну якість відновленої відеоінформації на прийнятному рівні;
- мінімізацію часу затримки на виконання кодування.

Водночас, аналіз принципів функціонування SRC свідчить про те, що даний алгоритм має ряд суттєвих недоліків, а саме:

- на випадок використання механізму балансування без адаптації параметрів, керування бітовою швидкістю виконується виключно на рівні групи кадрів, при цьому аналогічні параметри стиснення розповсюджуються на всі кадри у групі.

Відтак, деяка кількість кадрів групи може бути кодовано з невиправдано високою якістю, тоді як для інших кадрів може бути внесено суттєву помилку, що спричинює істотні втрати якості;

- прийнятна якість відео, а також мінімальна величина затримки забезпечуються в разі їх обробки для режиму низьких інтенсивностей;
- обмеження щодо роздільної здатності, часових інтервалів і діапазонів інтенсивностей застосування алгоритму SRC, що не дозволяє розглядати його як універсальний засіб для управління інтенсивністю відеоданих.

Ще одним підходом до балансування бітової швидкості відео є технологія ABR (adaptive bit-rate), що зараз використовується багатьма сервісами VoD. У рамках ABR на рівні файлоховища відео для одного джерела (вхідного файлу) створюється множина відеопотоків різних роздільних здатностей, що мають різні рівні бітової швидкості.

На базі даних потоків утворюється сукупність  $I$  прошарків якості, які, у свою чергу, підлягають поділу на часові відрізки  $t_{a,b}$ . Для цих відрізків справедливою є умова:

$$t(l)_b = t(a)_b = t(A)_b \quad (3)$$

Під час передавання  $b$ -го відеопотоку, якщо складаються умови, коли

$V(t) > B(t)$ , виконується вибір  $t(a-1)_b$ -го (наступного шижчого) прошарку якості за умови, що у поточний час транслюється  $t(a)_b$ -й, більш високий за якістю та бітовою швидкістю. У наслідок цього здійснюється ітераційний перехід до такого прошарку якості, коли забезпечується виконання умови  $V(t) \leq B(t)$ .

**До недоліків технології ABR можна віднести:**

- відсутність алгоритмів контролю та гарантування якості відео;
- надмірне завантаження файлоосховищ, що спричинюється необхідністю зберігання ряду відеофайлів різної роздільної здатності для кожного вихідного джерела;
- низька ефективність на випадок застосування для відеосервісів реального часу.

**Результати та обговорення.** За результатами розглянутого матеріалу можна констатувати доцільність реалізації механізмів балансування бітової швидкості відео потоку саме на рівні джерела. Це пояснюється як відсутністю недоліків, властивих технологіям ABR та механізмам балансування на рівні мережеских вузлів, так і можливістю застосування широкого інструментарію для оперативної зміни бітової швидкості у реальному часі. Це можуть бути усі механізми, що входять до базових технологій кодування у рамках MPEG у різних комбінаціях

**Висновки.** Виконано аналіз ряду поширених підходів до балансування бітової швидкості відеопотоку відносно динаміки пропускнуої спроможності мереж. Показано, що підходам до балансування бітової швидкості на рівні мережеских вузлів, та за рахунок створення сітки джерел відео різної бітової швидкості властивий ряд недоліків та обмежень, що не дозволяють їх розглядати у якості уніфікованих засобів.

Проте, найбільш ефективним є підхід, у рамках якого баланс бітової швидкості відео відносно пропускнуої спроможності досягається шляхом оперативної зміни параметрів кодування.

Для збільшення продуктивності цих методів може бути використано

динамічну зміну рівня структурних одиниць потоку, відносно яких виконується кодування, та одночасного застосування ряду технологічних процесів (наприклад, вибір формату колірної субдискретизації, квантування, сторонні механізми) для досягнення балансу бітової швидкості відносно пропускної спроможності.

