

СЕЛЕКТИВНИЙ МЕТОД ШИФРУВАННЯ ВИДЕОПОТОКУ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ НА ОСНОВІ ПРИХОВУВАННЯ БАЗОВОГО І-КАДРУ

Розглядається селективний метод шифрування відеокадрів, заснований на приховуванні базового І-кадру. Робота даного методу базується на основі обробки групи кадрів з урахуванням алгоритму MPEG, який реалізований за принципом формування послідовності відеокадрів різних типів. Представляються алгоритми і схеми кодування і декодування відеопотоку із застосуванням даного методу. Розробляється метод оцінки обсягу прихованого І-кадру і його стисненого подання без приховування щодо групи кадрів в процентному співвідношенні. Аналізується зміна обсягу стисненого уявлення групи кадрів з прихованим базовим кадром щодо стисненого початкового об'єму групи кадрів залежно від різних значень пікового відношення сигнал / шум для різних типів кадрів. Розробляється методологічна база для визначення різниці між обсягами стисненого уявлення групи кадрів із застосуванням приховування базового І-кадру і без приховування в процентному співвідношенні. Ключові слова: *відеокадр, група кадрів, обсяг кадру, шифрування, коефіцієнт стиснення, відношення сигнал/шум, зображення середньої насиченості, селективний метод.*

Вступ

Інтенсивні розробки систем телебачення високої роздільної здатності HDTV та стрімкий розвиток мультимедіа додатків останнім часом різко збільшили частку відеотрафіка в телекомунікаційних системах. Впровадження таких технологій набирає масову популярність серед користувачів Інтернету, в комерційних та державних організаціях. Тому виникає необхідність у розвитку механізмів та методів для організації конфіденційності інформації в телекомунікаційних системах (організація безпечного з'єднання та захист потокового відео, відеоконференцз'язку) [1-3]

Існуючі технології приховування відеоінформаційних ресурсів забезпечують необхідну конфіденційність. Однак вони мають істотний недолік: їх робота заснована на закритті усього потоку інформації, що передається незалежно від типу та змісту відеосцени. Такий підхід закриття інформації називається повним. Його використання для відкритих відеоінформаційних ресурсів в інфокомунікаційних системах реального часу є непрактичним. Це обумовлено такими причинами: уся структура відеоданих руйнується; у разі виникнення помилки в каналі передачі даних збільшується час обробки. Для вирішення цієї проблеми застосовується селективний підхід шифрування. Його суть полягає в приховуванні найбільш значущих компонент відеопотоку. Ці компоненти формуються в процесі стиснення відеоданих. Тому таке шифрування відноситься до селективного. Реалізація селективного підходу приховування можлива на різних рівнях формування MPEG-потoku. Ієрархія потоку включає в себе кілька рівнів: власне сам відеопотік (sequence), група кадрів (GOP -Group Of Pictures), слайс (slice), макроблок (macroblock) та блок (block). Пропонується закривати тільки базовий І-кадр. Це дозволить зменшити обсяг та час обробки шифрованих стислих відеоданих.

Розробка селективного методу шифрування відеопотоку

З урахуванням того, що вихідні обсяги всіх кадрів до обробки рівні, то формула для визначення обсягу стисненого представлення $V_{гк}^{(сж)}$ групи кадрів має вигляд [4]:

$$V_{гк}^{(сж)} = V_k \left(\frac{N_I}{K_I} + \frac{N_P}{K_P} + \frac{N_B}{K_B} \right), \quad (1)$$

де V_k – обсяг вихідного відеокадру; N_I – кількість І-кадрів у групі кадрів; N_P – кількість Р-кадрів у групі кадрів; N_B – кількість В-кадрів у групі кадрів; κ_I – коефіцієнт стиснення для І-кадрів; κ_P – коефіцієнт стиснення для Р-кадрів; κ_B – коефіцієнт стиснення для В-кадрів.

У випадку з закриттям І-кадру його структура руйнується – знижується потенційна кількість статистичної, психовізуальної та структурної надлишковості, аж до нульового рівня. У результаті цього зменшується коефіцієнт стиснення $\kappa_{I,3}$ для І-кадру. Обсяг закритого І-кадру визначається величиною $V_{I,3}^{(сж)}$. Відповідно, обсяг стисненого представлення групи кадрів $V_{гк,3}^{(сж)}$, що містить закритий І-кадр, розраховується за формулою:

$$V_{гк,3}^{(сж)} = V_k \left(\frac{N_I}{\kappa_{I,3}} + \frac{N_P}{\kappa_P} + \frac{N_B}{\kappa_B} \right). \quad (2)$$

Оцінимо зміни обсягу групи кадрів з приховуванням $V_{гк,3}^{(сж)}$ та без приховування $V_{гк}^{(сж)}$ базового І-кадру. Для цього необхідно знати коефіцієнти стиснення для реалістичного середньонасиченого кадру при певних значеннях PSNR пікового відношення сигнал/шум.

Для розрахунку ступеня стиснення різних типів кадрів використовуються такі значення:

– для визначення коефіцієнта стиснення κ_I для І-кадрів використовується пікове відношення сигнал/шум PSNR = 50; 45; 40 дБ. Великі значення задаються для збереження високого деталювання І-кадрів. Тому для них задаються таблиці квантування з найменшими коефіцієнтами. Також І-кадри мають найменшу ступінь стиснення через застосування алгоритмів тільки всередині кадрового передбачення;

– для визначення коефіцієнта стиснення κ_P для Р-кадрів використовується пікове відношення сигнал/шум PSNR = 40; 35; 30 дБ. Це пов'язано з тим, що Р-кадри несуть менше візуального навантаження. При їх кодуванні застосовуються алгоритми компенсації руху та міжкадрового передбачення за попередніми І- або Р-кадрами. Для Р-кадрів задаються таблиці квантування з середніми коефіцієнтами;

– для визначення коефіцієнта стиснення κ_B для В-кадрів використовується пікове відношення сигнал/шум PSNR = 30; 25; 23 дБ. В процесі їх формування застосовуються алгоритми компенсації руху і двонаправленого передбачення за попередніми та наступними І- або Р-кадрами. Для них задаються таблиці квантування з найбільшими коефіцієнтами. Тому ступінь стиснення для В-кадрів є максимальною в порівнянні з іншими типами відеокадрів.

Проведемо розрахунок обсягу $\Delta V_I^{(сж)}$ стисненого представлення І-кадру щодо обсягу групи кадрів у процентному співвідношенні з урахуванням виразів (1) і (2):

$$\Delta V_I^{(сж)} = \frac{100\%}{1 + \frac{\kappa_I}{\kappa_P} N_P + \frac{\kappa_I}{\kappa_B} N_B}. \quad (3)$$

Значення обсягу $\Delta V_{I,3}$ прихованого І-кадру щодо обсягу груп кадрів у процентному співвідношенні розраховується так:

$$\Delta V_{I,3} = \frac{100\%}{1 + \frac{\kappa_{I,3}}{\kappa_P} N_P + \frac{\kappa_{I,3}}{\kappa_B} N_B}. \quad (4)$$

Значення приросту обсягу $V(h_I; h_P; h_B)$ прихованого кадру щодо обсягу стисненого неприхованого кадру в групі кадрів у процентному співвідношенні розраховується за формулою:

$$V(h_I; h_P; h_B) = \Delta V_I^{(сж)} - \Delta V_{I,3}. \quad (5)$$

На рис. 1 зображена діаграма залежності значень обсягів стисненого представлення I-кадру та значень обсягів прихованого I-кадру щодо обсягу групи кадрів у процентному співвідношенні.

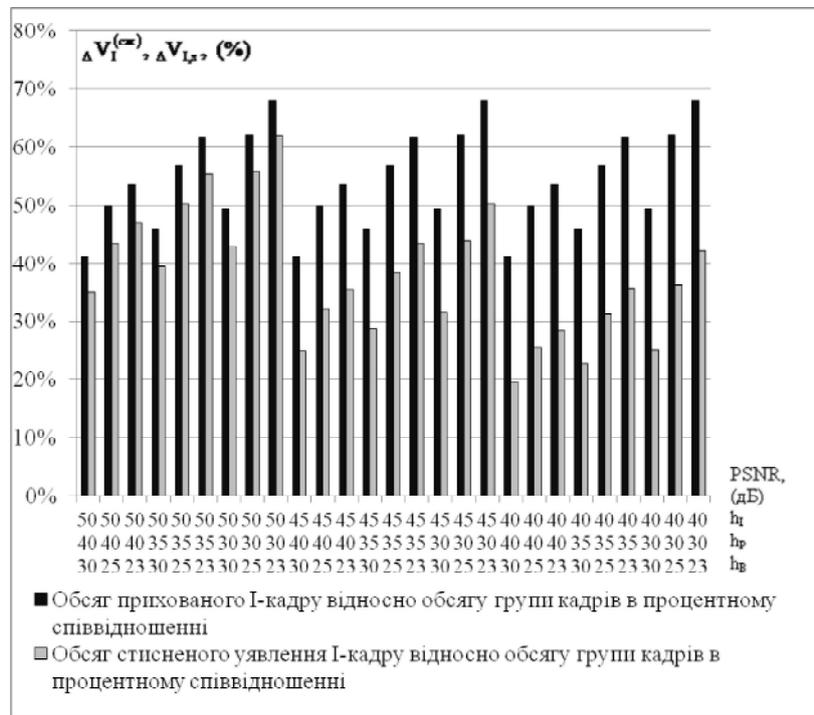


Рис. 1. Діаграма значень обсягу $\Delta V_{I,3}$ стисненого представлення I-кадру і прихованого обсягу $\Delta V_I^{(сж)}$ I-кадру залежно від пікового відношення сигнал/шум в групі кадрів у процентному співвідношенні

З розрахунків видно, що приріст обсягу прихованого кадру у процентному співвідношенні щодо обсягу стисненого неприхованого кадру в групі кадрів залежно від значень PSNR становить 7 - 25%. Це обумовлено утаєнням базового I-кадру щодо варіанту стиснення I-кадру без приховування.

З аналізу діаграми на рис. 1 видно, що обсяг прихованого I-кадру більше обсягу стисненого представлення I-кадру щодо обсягу групи кадрів у процентному співвідношенні. Також видно, що зі зниженням значень пікового відношення сигнал/шум вага (у відсотках) прихованого I-кадру в групі кадрів збільшується. Це пов'язано з тим, що при низьких значеннях PSNR для P- та B-кадрів ступінь стиснення збільшується, а для прихованого I-кадру - ступінь стиснення є постійним ($\kappa_I = 1$). Розрахунки показали, що при високих значеннях PSNR обсяг стисненого представлення I-кадру становить 35% від усього обсягу групи кадрів, а обсяг прихованого I-кадру в групі кадрів склав 42%. При низьких значеннях PSNR обсяг стисненого представлення I-кадру щодо обсягу групи кадрів дорівнює 43%, а прихованого I-кадру - 68%.

У селективному підході прихованню піддається тільки I-кадр, який є базовим та має максимальний обсяг у групі кадрів. Тому зі зменшенням значень пікового відношення сигнал/шум ступінь стиснення для I-кадру буде постійним ($\kappa_I = 1$), а для P та B кадрів ступінь стиснення буде рости. У результаті цього обсяг I-кадру щодо обсягу групи кадрів у процентному співвідношенні з застосуванням селективного шифрування залежно від пікового відношення сигнал/шум може коливатися від 41 до 68%.

Також слід відзначити те, що при використанні алгоритмів шифрування після квантування структура проміжного представлення руйнується. Змінюються структурні характерис-

тики (значення компонент та залежність між ними) в матрицях дискретного косинусного перетворення. Це руйнує імовірнісні та статистичні характеристики, призводить до відсутності ланцюжків нульових значень при зигзаг-скануванні, в результаті чого ступінь стиснення I-кадру зменшується. Тому відмінності між значеннями обсягів стисненого представлення групи кадрів з утаєнням базового I-кадру та без приховування у процентному співвідношенні стають явно вираженими та можуть досягати 35%.

Для визначення зміни візуальної якості зображень при різних режимах обробки проведемо оцінку середніх значень пікового відношення сигнал/шум $PSNR(8)_{cp}$ для 8 відеокадрів середньонасичених зображень, які визначаються так:

$$PSNR(8)_{cp} = \frac{PSNR(K_I) + 2 \cdot PSNR(K_B) + 5 \cdot PSNR(K_P)}{8} \quad (6)$$

Залежність середнього значення пікового відношення сигнал/шум у групі з 8 кадрів для середньонасичених зображень від коефіцієнтів стиснення при різних режимах обробки розрахована за формулою (6) та представлена у вигляді діаграми на рис. 2.

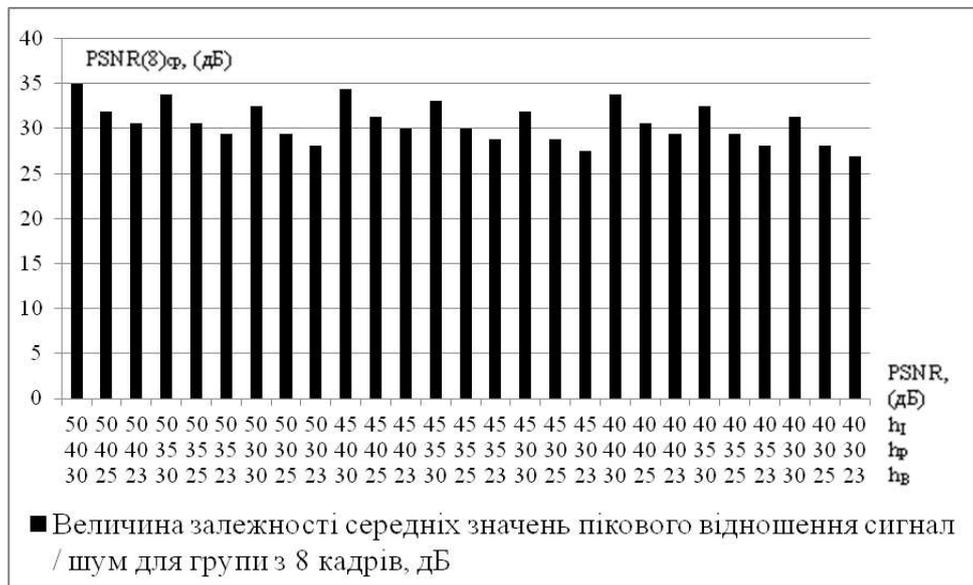


Рис. 2. Середні значення $PSNR(8)_{cp}$ по групі з 8 кадрів для різних режимів обробки кадрів у середньонасичених зображеннях

З аналізу діаграми на рис. 2 видно, що:

- середні значення для групи з 8 кадрів при різних режимах обробки кадрів у середньонасичених зображеннях коливаються в межах 27-35дБ. Це свідчить про значні зміни якості зображень при різних режимах обробки;
- при зміні PSNR для I-кадру на 5дБ середнє пікове значення відношення сигнал/шум для групи кадрів зменшується на 1дБ. При цьому такі зміни незначно впливають на обсяг стисненого представлення групи кадрів;
- на середній PSNR групи кадрів суттєво впливають значення відношення сигнал/шум для P- та B-кадрів.

На рис. 3 зображена діаграма приросту обсягу $D(h_I; h_P; h_B)$ стисненого представлення групи кадрів у процентному співвідношенні з застосуванням приховування базового I-кадру та без приховування залежно від середнього пікового відношення сигнал/шум для середньонасичених зображень.



Рис. 3. Діаграма приросту $D(h_I; h_P; h_B)$ стисненого представлення обсягу групи кадрів з прихованим I-кадром відносно стисненого представлення обсягу групи кадрів без приховування в процентному співвідношенні з урахуванням середніх значень пікового відношення сигнал/шум для середньонасичених зображень

На діаграмі (див.рис.3) чітко спостерігається збільшення приросту обсягу стисненого представлення обсягу $V_{ГК}^{сж,3}$ групи кадрів з прихованим базовим I-кадром по відношенню до стисненого подання обсягу $V_{ГК}^{сж}$ групи кадрів без приховування зі зменшенням середнього пікового відношення сигнал/шум для групи кадрів. Видно, що при зменшенні середнього PSNR для групи кадрів на 9 дБ приріст обсягу $D(h_I; h_P; h_B)$ стисненого представлення $V_{ГК}^{сж,3}$ групи кадрів з прихованим базовим I-кадром по відношенню до стисненого подання обсягу $V_{ГК}^{сж}$ групи кадрів без приховування досягає 35%.

Висновки

1. Розроблено метод селективного шифрування в процесі стиснення відеопотоку, заснований на приховуванні базового I-кадру. Робота даного методу базується на основі обробки групи кадрів, з урахуванням алгоритму MPEG, який реалізований за принципом формування послідовності відеокадрів різних типів. В результаті його роботи ховається весь відеопотік при шифруванні від 8% до 15% початкового об'єму відеоданих. Даний метод шифрування застосовується після етапу квантування. Наукова новизна - пропонується метод приховування відеопотоку, заснований на шифруванні тільки базового I-кадру. Це дозволяє забезпечити приховування групи кадрів в умовах мінімізації втрат за ступенем стиснення. Він враховує ступінь стиснення в процесі кодування в залежності від пікового відношення сигнал/шум. У роботі представлена схема і алгоритм кодування відеопотоку в селективному підході з приховуванням I-кадру.

2. Розроблено метод оцінки обсягу прихованого I-кадру та його стисненого подання без приховування щодо групи кадрів у процентному співвідношенні. Проведено аналіз зміни обсягу стисненого представлення I-кадру та прихованого обсягу I-кадру щодо групи кадрів у процентному співвідношенні. Його результати показали, що залежно від пікового відношення сигнал/шум обсяг прихованого I-кадру в порівнянні зі стисненим його поданням щодо групи кадрів збільшується від 7 до 20%.

3. Розроблена методологічна база для визначення різниці між обсягами стисненого представлення групи кадрів із застосуванням приховування базового I-кадру та без приховування у процентному співвідношенні. Проведено розрахунки щодо зміни обсягу стиснено-

го представлення групи кадрів з прихованим I-кадром та без його приховування. Вони показали, що зі зменшенням пікового відношення сигнал/шум обсяг стисненого представлення групи кадрів з прихованим I-кадром збільшується з 9 до 44% відносно обсягу стисненого представлення групи кадрів без приховування I-кадру.

Список літератури: 1. *Ватолін Д., Ратушняк А., Смирнов М., Юкин В.* Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео. М.: Диалог-Мифи, 2003. 381 с. 2. *Ян Ричардсон.* Видеокодирование. H.264 и MPEG-4 — стандарты нового поколения. М.: Техносфера, 2005. 368 с. 3. *Баранник В.В.* Кодирование трансформированных изображений в инфокоммуникационных системах / В.В. Баранник, В.П. Поляков. Х.: ХУПС, 2010. 212 с. 4. *Баранник В.В.* Методологическая база для управления битовой скоростью видеопотока в процессе компрессии / Баранник В.В. // Праці УНДІРТ. 2013. 22с.

Надійшла до редколегії 09.09.2015

Баранник Володимир Вікторович, д-р техн. наук, професор, начальник кафедри Харківського університету Повітряних Сил ім. І. Кожедуба. Наукові інтереси: системи, технології перетворення, кодування, захисту та передачі інформації, семантичної обробки зображень. Адрес: Україна, 61023, Харків, 23, вул. Сумська, 77/79.

Комолов Дмитро Іванович, пошукач Харківського національного університету радіоелектроніки. Наукові інтереси: системи, технології перетворення, кодування, захисту та передачі інформації, семантичної обробки зображень. Адрес: Україна, 61166, Харків, пр. Науки, 14.