

УДК 621.397

Д.С. Гаврилов¹, О.В. Бойко¹, Д.А. Тарасенко²¹ Харківський національний університет Повітряних Сил ім. І. Кожедуба, Харків² Черкаський державний технологічний університет, Черкаси

КЛАСТЕРНЕ КОДУВАННЯ БІТОВОГО ПОТОКУ В ЗАЛЕЖНОСТІ ВІД СТРУКТУРИ ВХІДНИХ ДАНИХ

В роботі запропонований підхід обробки даних з використанням кластерного кодування в залежності від бітового потоку, який надходить. Обґрунтовано використання розробленого адаптивного алгоритму RLE-кодування та адаптивного арифметичного кодування.

Ключові слова: обробка, адаптивне RLE-кодування, адаптивне арифметичне кодування, оперативність.

Вступ

Постановка проблеми. Як у відомчих, так і в комерційних структурах безупинно намагаються збільшити оперативність та конфіденційність передачі даних усунувши затримку. Дане намагання викликано тим, що у визначених структурах курсує інформація, яка при потраплянні до несанкціонованого користувача може призвести до економічних, політичних та соціальних втрат. Необхідний рівень конфіденційності досягається за допомогою використання криптографічних алгоритмів, які, як правило, пройшли атестацію та є стандартами. На даний час на території України в якості стандарту діє алгоритм симетричного блочного шифрування «Калина», який був прийнятий в національному стандарті України ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блочного перетворення» від 1 липня 2015 р. Даний документ дозволяє використовувати алгоритм «Калина» у відомчих телекомунікаційних системах України. Що стосується оперативної передачі даних, то пропонується використовувати алгоритми компресії, які дозволять за рахунок усунування надлишковостей зменшити об'єм, а отже і час на передачу даних. Проте, різні алгоритми компресії в залежності від виду вхідних даних дають різні коефіцієнти компресії, в деяких випадках навіть збільшуючи початковий об'єм. Тому, актуальною науково-прикладною задачею є відшукування алгоритмів компресії, які б обиралися в залежності від вхідних даних та давали максимальний коефіцієнт компресії з забезпеченням необхідної якості.

Аналіз останніх досліджень і публікацій. Беручи за основу публікацію [9], в якій вказано, що від ступеня насиченості зображення залежить частка «1» та «0» в трансформанті вважаємо можливим та необхідним використовувати алгоритми компресії, які в залежності від особливостей даних, що поступають будуть давати найбільші коефіцієнти компресії

збереженням необхідного рівня якості. Завдяки даним маніпуляціям можливо забезпечити оперативну передачу даних, яка вимірюється часом $T_{\text{дов}}$ доведення:

$$T_{\text{дов}} = \frac{V}{\delta}, \quad (1)$$

де V – об'єм даних, які мають бути передані;
 δ – пропускна спроможність каналу зв'язку.

Очевидно, що для оперативної роботи системи передачі даних необхідне виконання умови $T_{\text{дов}} \rightarrow \min$. При цьому можливі наступні шляхи задоволення даної потреби:

- 1) коли об'єм даних, що передаються буде мінімальним, при збереженні необхідної якості ($V \rightarrow \min$);
- 2) коли пропускна спроможність каналу буде максимальна, що дозволить «миттєво» передавати дані будь-якого об'єму ($\delta \rightarrow \max$);
- 3) комбінований, при якому $V \rightarrow \min$ та $\delta \rightarrow \max$.

В даній роботі другий шлях не розглядається, так як відшукування такого каналу, який задовольнить потреби користувачів без використання алгоритмів обробки, вважаємо неможливим.

Формулювання мети статті. Завданням дослідження є відшукування шляху задоволення потреби $V \rightarrow \min$ за рахунок використання алгоритмів компресії, які дозволять досягти максимальної величини коефіцієнта компресії $K_{\text{комп}}$ без суттєвої втрати якості (не більше допустимих). Коефіцієнт компресії $K_{\text{комп}}$ розраховується як відношення вихідного об'єму $V_{\text{вих}}$ до об'єму $V_{\text{ст}}$ стиснутих даних:

$$K_{\text{комп}} = \frac{V_{\text{вих}}}{V_{\text{ст}}}. \quad (2)$$

Даний підхід дозволить задовольнити потребу

в оперативній передачі даних $T_{\text{дов}} \rightarrow \min$.

Виклад основного матеріалу

Дані дослідження викладені в публікації [9] свідчать про різну ймовірність появи елементів в залежності від ступеня насиченості блоку контурною інформацією (табл. 1).

Таблиця 1

Результати дослідження ймовірності появи елементу в трансформанті

клас блоку	без контурної інформації	з поступовим переходом	з контурною інформацією
розмір блоку	8 x 8	8 x 8	8 x 8
ймовірність появи «1»	0,0059	0,2928	0,4761
ймовірність появи «0»	0,9941	0,7072	0,5239
відношення "1" до "0" (K), %	0,5935	41,4027	90,8761

В результаті проведеного дослідження (табл. 1) запропоновано блок-схему вибору алгоритму кодування в залежності від ймовірності P_1 появи елемента рівному «1» та ймовірності P_0 появи елемента рівному «0» (рис. 1).

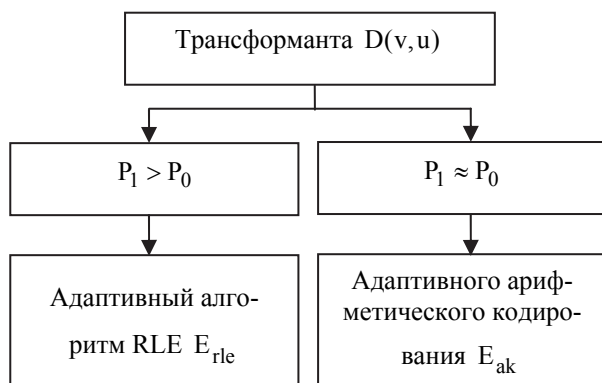


Рис. 1. Блок-схема вибору алгоритму кодування в залежності від ймовірності появи елементів що поступають

Для компресії бітового потоку при $P_1 > P_0$, пропонується використовувати адаптивний алгоритм RLE E_{rle} (рис. 2). Адаптація алгоритму полягає у тому, що стандартна пара «кількість повторень, значення елемента» замінена на 8-ми бітове число, в якому старший біт відводиться на «значення елемента» (так як на вхід може поступити лише

«0» або «1»), а решта 7 біт вказують на кількість повторень (довжину серії).

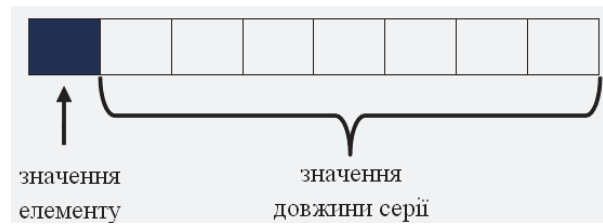


Рис. 2. Формат коду після адаптивного RLE кодування

Слід відмітити, що при використанні запропонованого алгоритму максимальне значення довжини серії може бути $2^7 = 127$.

Приклад:

Нехай кодується серія виду:

$$S = |0_1 0_2 \dots 0_{99} 0_{100} 1_1 1_2 \dots 1_{79} 1_{80}|.$$

Використовуючи адаптивний алгоритм RLE E_{rle} вектор-код прийме наступний вигляд:

$$E_{rle}(S) = |100; 208|.$$

В двійковому вигляді код буде наступний:

$$E_{rle}(S)_2 = |01100100; 11010000|.$$

Об'єм отриманого коду $V_{cr} = 16$. Об'єм вихідного масиву трансформанти дорівнює $V_{вих} = 180$. Виходячи з цих даних коефіцієнт компресії, для даного масиву, дорівнює $K_{комп} = 11,25$.

Для компресії бітового потоку при $P_1 \approx P_0$, пропонується використовувати адаптивний алгоритм арифметичного кодування E_{ak} . Даний метод простий в реалізації та має високий рівень швидкодії за рахунок простих розрахунків, які полягають у визначенні інтервалу в якому знаходиться кодовий елемент (рис. 3):

$$E_{ak} = \frac{l_f + h_f}{2},$$

де l_f – початок робочого інтервалу f-го кодованого символу;

h_f – кінець робочого інтервалу f-го кодованого символу;

Приклад:

Нехай кодується серія виду:

$$S = |0 0 1 0 1 1 1 0|.$$

Спочатку будується табл. 2.

Сума ваги на f-ом кроці визначається за виразом:

$$\eta_f = \eta_0 + \eta_1,$$

де η_0 – вага «0»;
 η_1 – вага «1».

Таблиця 2

Таблиця вихідних даних для арифметичного кодування

№ кроку	значення елемента, який кодується	вага η		наявна величина інтервалу	робочий інтервал $[l_f; h_f]$
		«0»	«1»		
		1	1		
1	0	2	1	1	[0; 1]
2	0	3	1	0,5	[0; 0,5]
3	1	3	2	0,33	[0; 0,33]
4	0	4	2	0,163	[0,167; 0,33]
5	1	4	3	0,0815	[0,167; 0,2485]
6	1	4	4	0,0465	[0,2019; 0,2485]
7	1	4	5	0,02913	[0,2194; 0,2485]
8	0	5	5	0,0161	[0,2323; 0,2484]

Величину сегмента на f-ом кроці можна виразити за формулою:

$$\rho_f = \frac{h_f - l_f}{\eta_f}$$

При кодуванні «0» робочий інтервал $[l_f; h_f]$ можна знайти за допомогою виразу:

$$l_f = l_{f-1};$$

$$h_f = l_f + \eta_f^0 \cdot \rho_f,$$

де l_{f-1} – початок робочого інтервалу попереднього кодованого символу;

η_f^0 – вага «0» на f-му кроці.

При кодуванні «1» робочий інтервал $[l_f; h_f]$ можна знайти за допомогою виразу:

$$h_f = h_{f-1};$$

$$l_f = h_f - \eta_f^1 \cdot \rho,$$

де η_f^1 – вага «1» на f-ому кроці.

В результаті адаптивного арифметичного кодування (рис. 3) отримуємо робочий інтервал [0,2323; 0,2404] для даного інтервалу кодоване значення прийме вид:

$$E_{ak} = |11000|.$$

Маючи дане значення можна безпомилково ві-

дтворити всю кодовану послідовність, таким чином, інформація про межі даного інтервалу є конфіденційна.

Після проведення кластерного кодування для підвищення захисту даних, які передаються пропонується проводити криптозахист відомостей про спосіб кодування.

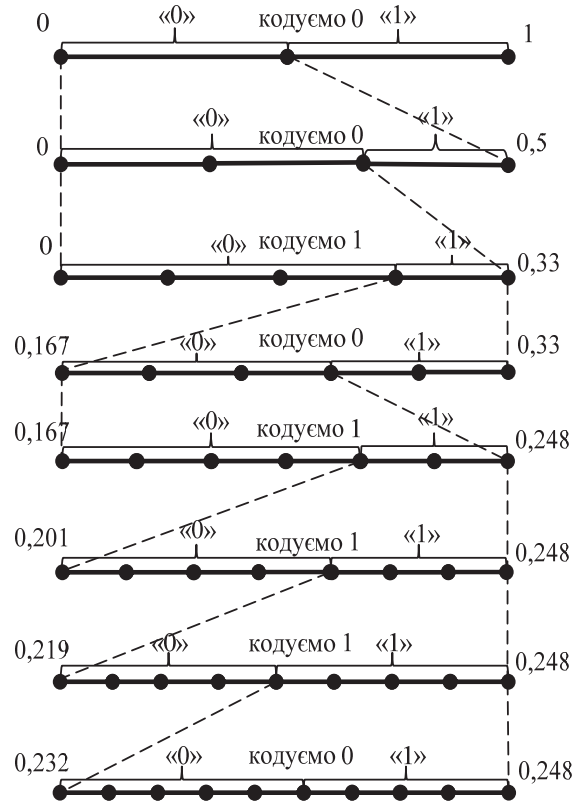


Рис. 3. Процес побудови коду адаптивним арифметичним кодуванням

Висновки

Розроблений підхід в системі кластерної обробки бітового потоку забезпечить оперативність передачі даних. За рахунок криптозахисту відомостей про спосіб кодування пропонується підвищити захист передачі даних.

Наукова новизна. Вперше розроблений алгоритм адаптивного RLE-кодування, який оперуючи вхідним бітовим потоком дозволить досягти значної величини коефіцієнта компресії при збереженні якості.

Список літератури

1. Barannik V.V. The model of avalanche-relating effect in the process of images reconstruction in the combined cryptosemantic systems on the polyadic presentation / V.V. Barannik V.V. Larin, S.A. Sidchenko // Наукоємні технології. – 2010. – № 1(5). – С. 68-70.
2. Gavrilov D. The analysis of template method of video processing / V. Larin, P. Krasnikov, D. Gavrilov // Proceedings of 2015 1st International Conference on Advanced Information and Communication Technologies-

2015 (AICT'2015), Lviv, Ukraine, October 29 – November 1, 2015. – P. 87-89.

3. Баранник В.В. Метод підвищення інформаційної безпеки в системах відеомоніторингу кризових ситуацій: моногр. / В.В. Баранник, Ю.Н. Рябуха. – Черкаси, 2015. – 143 с.

4. Баранник В.В. Модель загроз безпеки відеоінформаційного ресурсу систем відеоконференцзв'язку / А.В. Власов, В.В. Баранник, Р.В. Тарнополов // Наукоємні технології. – 2014. – № 1 (21). – С. 55-60.

5. Обоснование значимых угроз безопасности видеоинформационного ресурса систем видеоконференцсвязи профильных систем управления / В.В. Баранник, А.В. Власов, С.А. Сидченко, А.Э. Бекиров // Информационно-управляющие системы на ЖД транспорте. – 2014. – № 3. – С. 24-31.

6. Баранник В.В. Селективний метод шифрування відеопотоку в телекомунікаційних системах на основі приховування базового І-кадру / В.В. Баранник, Д.І. Комолов, Ю.М. Рябуха // Наукоємні технології. – № 2. – 2015. – С. 14-23.

7. Методология совершенствования обработки видеоинформации, для повышения эффективности сервиса предоставления дистанционных видеослужб, при управлении в кризисных ситуациях / В.В. Баранник, Ю.Н. Рябуха, А.А. Красноруцкий, В.Ж. Яценко // АСУ и приборы автоматики. – 2015. – № 170. – С. 12-20.

8. Метод захисту низькочастотних складових в алгоритмі кодування JPEG / В.В. Ларин, Д.С. Комолов, К.В. Ялівець, Д.С. Гаврилов // Системи обробки інформації. – 2015. – № 9 (134). – С. 121-123.

9. Метод забезпечення безпеки відеоінформаційного ресурсу на основі багаторівневої селективної обробки в телекомунікаційних системах / О.Г. Оксіюк, Д.С. Гаврилов, П.М. Гуржій, Б.О. Демідов // Наука і техніка Повітряних Сил Збройних Сил України. – 2017 – № 1. – С. 46-48.

Надійшла до редколегії 12.06.2017

Рецензент: д-р техн. наук проф. В.В. Баранник, Харківський національний університет Повітряних Сил ім. І. Кожеду-ба, Харків.

КЛАСТЕРНАЯ КОДИРОВКА БИТОВОГО ПОТОКА В ЗАВИСИМОСТИ ОТ СТРУКТУРЫ ИСХОДНЫХ ДАННЫХ

Д.С. Гаврилов, О.В. Бойко, Д.А. Тарасенко

В работе предложен подход обработки данных с использованием кластерной кодировки в зависимости от входящего битового потока. Обосновано использование разработанного адаптивного алгоритма RLE-кодировки и адаптивной арифметической кодировки.

Ключевые слова: обработка, адаптивное RLE-кодирования, адаптивное арифметическое кодирование, оперативность.

CLUSTER CODING BIT STREAM DEPENDING ON THE STRUCTURE OF THE SOURCE DATA

D. Havrylov, O. Boyko, D. Tarasenko

In this paper, the proposed approach processing using cluster encoding depending on the incoming bitstream. The use of the developed adaptive algorithm RLE-coding and adaptive arithmetic coding is grounded.

Keywords: processing, adaptive RLE-coding, adaptive arithmetic coding efficiency.