

С. Г. Семенов, О. В. Липчанська, М. В. Липчанський

Національний технічний університет «ХПИ», Харків

УДОСКОНАЛЕННЯ ПРОЦЕСУ ДЕКОДУВАННЯ МУЛЬТИМЕДІА ДАНИХ, ЗАКОДОВАНИХ АЛГОРИТМОМ ШОКРОЛАХІ

Предметом вивчення в статті є процеси передавання даних в системах критичного застосування. **Метою** є розробка вдосконаленого алгоритму декодування мультимедіа даних, закодованих завадостійким фонтанним кодом Шокролахі. **Задачі**: підвищити достовірність і оперативність декодування мультимедіа даних, переданих по бездротових каналах зв'язку, розглянути існуючі алгоритми кодування і декодування Шокролахі для передачі мультимедіа даних по каналах зі стиранням, адаптувати існуючий код до підвищених вимог оперативності та достовірності шляхом удосконалення процедури декодування відеоінформації, провести порівняльний аналіз ефективності роботи запропонованої процедури по відношенню до існуючої стандартної процедур . **Використаними методами** є: фонтанний код Шокролахі, метод Гауса, алгоритм поширення довіри, LT код. Отримані наступні результати: сформульовано задачу підвищення достовірності і оперативності декодування мультимедіа даних, удосконалено процедуру декодування мультимедіа даних, закодованих фонтанним кодом Шокролахі, показана ефективність роботи даної процедури у порівнянні з існуючим алгоритмом декодування. **Висновки**: наукова новизна отриманих результатів полягає в наступному: ми вдосконалили стандартну процедуру декодування Шокролахі шляхом організації можливості продовжувати декодування при виникненні збою з моменту збою, не повертаючись до початку першого етапу. Виграш у часі становить від 1,3 до 1,7 разів в залежності від розміру переданих символів і кількості символів в кодованих блоках. Отриманий результат є важливим в силу того, що час є однією з основних характеристик показників якості при передаванні даних.

Ключові слова: фонтанні коди; декодування мультимедіа даних; системи критичного застосування; оперативність і достовірність передавання даних.

Вступ

На сьогоднішній день в Україні задача забезпечення захисту інфраструктури критичного застосування від різних видів загроз і їх комбінацій є актуальною і важливою [1 – 5]. Одним з найбільш важливих об'єктів критичної інфраструктури України є залізничний транспорт. У нормативних документах, що відносяться до управління залізничним транспортом [6, 7], зафіксовано, що основними принципами забезпечення безпеки є вдосконалення системи управління безпекою руху поїздів шляхом впровадження сучасних комп'ютерних інформаційних технологій і засобів. Одним з таких шляхів є використання систем відео контролю на найбільш важливих ділянках руху залізничного транспорту із надсиланням відеоданих на засоби відображення у кабіні машиніста. Розглянутий тип даних вимагає передачі із заданою якістю забезпечення послуг. При цьому однією з основних характеристик якості послуг, що надаються при передачі мультимедійних даних є достовірність і оперативність.

Актуальність. Аналіз літературних джерел [8 – 10] показав, що в даний час питання підвищення оперативності і достовірності передачі мультимедійних даних залишаються актуальними та їм приділяється багато уваги фахівців. Так в роботах [11, 12] вирішення завдання якісної передачі відеоінформації пов'язують із використанням фонтанних кодів. Це дозволяє відправляти дані по каналах зв'язку з низькими якісними характеристиками і відновлювати інформаційні пакети у разі втрати частини з них. Це дає можливість не покладатися на знання рівня втрати пакетів. Проведені дослідження [11 – 14] показали, що в умовах використання переважно методів і засобів бездротового зв'язку для забезпе-

чення якості передачі мультимедійної інформації, найбільш ефективним є фонтанний код Шокролахі, в першу чергу це пов'язано з можливістю його практичної реалізації, відносно невеликого часу кодування, а також його здатності відновити пакет цілком у разі його втрати.

Однак в умовах постійного зростання швидкостей рухомого складу залізничного транспорту, динамічної зміни навколо транспортної обстановки, а також наявності об'єктивно існуючих факторів зниження вірогідності передачі мультимедіа даних дуже важливим завданням залишається адаптація існуючих кодів до підвищених вимог оперативності та достовірності.

Тому актуальним завданням є удосконалення існуючих методів і алгоритмів кодування Шокролахі та їх адаптація до підвищених вимог оперативності і достовірності при передачі мультимедійної інформації.

Виклад основного матеріалу

1. Опис стандартних процедур кодування та декодування кодом Шокролахі.

Принцип коду Шокролахі полягає в кодуванні по одному блоку вихідних символів, розмір кожного вихідного символу l лежить в межах від 1 до 1024 байт. Різні блоки вихідних символів можуть складатися з різної кількості K вихідних символів [15].

Кодування інформації кодом Шокролахі проводиться в два етапи.

На першому етапі процесу кодування відбувається отримання попереднього зовнішнього коду A – попереднього коду, який представляє собою двійкову матрицю, що складається із породжувальної матриці з низькою щільністю перевірки на парність

(G_{LDPC}), яка породжує матриці з високою щільністю перевірки на парність (G_{Half}) і матриці LT (G_{LT}).

Попередній код $[A]_{L \times L}$ виконує дві функції. Матриці A , G_{LDPC} і G_{Half} гарантують, що кожен вихідний символ кодується, щонайменше, один раз, і це дозволяє декодеру відновити кожен вихідний символ. Попередній код $[A]_{L \times L}$ містить перші K рядків породжувальної матриці $[G_{LT}]_{N \times L}$, що означає, що перші K вихідних символів LT-кодера відповідають K вихідним символам.

В першу чергу кодер кодує K вихідних символів $S[j]$, $j = 0, \dots, K-1$ в L проміжних символи $C[i]$, $i = 0, \dots, L-1$, використовуючи попередній код A . Символи $C[i]$, згенеровані G_{LDPC} і G_{Half} , називаються надлишковими символами і обчислюються за виразом (1).

$$\begin{bmatrix} C[0] \\ \vdots \\ C[L-1] \end{bmatrix}_{[C]_{L \times 1}} = \begin{bmatrix} [G_{LDPC}]_{S \times K} & I_{S \times S} & Z_{S \times H} \\ [G_{Half}]_{H \times (K+S)} & I_{H \times H} & \\ [G_{LT}]_{K \times L} & & \end{bmatrix}_{[A]_{L \times L}}^{-1} \cdot \begin{bmatrix} Z_{S \times 1} \\ Z_{H \times 1} \\ S[0] \\ \vdots \\ S[k-1] \end{bmatrix}_{[S_R]_{L \times 1}}, \quad (1)$$

де S – кількість LDPC символів, H – кількість Half символів, L – кількість проміжних символів, $L = K + S + H$.

На другому етапі кодування відбувається отримання внутрішнього коду Лабі. При цьому застосовується кодувальник LT коду, який використовує проміжні символи для генерації N закодованих символів $E[i]$, $i = 0, \dots, N-1$, $N \geq K$, відповідно до виразу (2).

$$\begin{bmatrix} E[0] \\ \vdots \\ E[N-1] \end{bmatrix}_{[E]_{N \times 1}} = \begin{bmatrix} g_{11} & \dots & g_{1L} \\ \vdots & \ddots & \vdots \\ g_{N1} & \dots & g_{NL} \end{bmatrix}_{[G_{LT}]_{N \times L}} \cdot \begin{bmatrix} C[0] \\ \vdots \\ C[L-1] \end{bmatrix}_{[C]_{L \times 1}}, \quad (2)$$

де N – кількість закодованих символів і $N = K(1 + \epsilon)$, ϵ – надмірність кодування в процентах.

Кожному закодованому символу присвоюється власний ідентифікатор.

Підматриця $[G_{LT}]_{K \times L}$ з матриці A включається в якості перших K рядків $[G_{LT}]_{N \times L}$, що призводить до того, що перші K закодованих символів відповідають K вихідним символам, тобто $E[i] = S[i]$, для $i = 0, \dots, K-1$.

Процес декодування також виконується в два етапи [15]. На першому етапі для відновлення проміжних символів $C[j]$, $j = 0, \dots, L-1$ необхідно отримати попередній код $[A]_{M \times L}$, використовуючи N' отриманих закодованих символів ($N' \geq K$), де M – кількість рядків в попередньому коді A , $M = S + H + N'$, як показано у виразі (3). Перші $S + H$ рядків в попередньому коді $[A]_{M \times L}$ відповідають рядкам в матриці A з виразу (1). Для N' прийнятих закодованих символів генерується підматриця $[G_{LT}]_{N' \times L}$ із використанням значень ідентифікаторів закодованих символів. Рядки в підматриці $[G_{LT}]_{N' \times L}$, відповідні втраченим закодованим символам, виключені з підматриці $[G_{LT}]_{N' \times L}$.

$$\begin{bmatrix} [G_{LDPC}]_{S \times K} & I_{S \times S} & Z_{S \times H} \\ [G_{Half}]_{H \times (K+S)} & I_{H \times H} & \\ [G_{LT}]_{N' \times L} & & \end{bmatrix}_{[A]_{M \times L}} \cdot \begin{bmatrix} C[0] \\ \vdots \\ C[L-1] \end{bmatrix}_{[C]_{L \times 1}} = \begin{bmatrix} Z_{S \times 1} \\ Z_{H \times 1} \\ E'[0] \\ \vdots \\ E'[N'-1] \end{bmatrix}_{[D]_{M \times 1}}, \quad (3)$$

де D містить отримані закодовані символи для $i = 0, \dots, S + H - 1$ і нульові символи для $i = S + H, \dots, M$.

На другому етапі процесу декодування після отримання проміжних символів відбувається відновлення K вихідних символів $S[j]$ для $j = 0, \dots, K-1$, з використанням породжувальної матриці LT розміром $K \times L$:

$$\begin{bmatrix} S[0] \\ \vdots \\ S[K-1] \end{bmatrix}_{[S]_{K \times 1}} = \begin{bmatrix} g_{11} & \dots & g_{1L} \\ \vdots & \ddots & \vdots \\ g_{N1} & \dots & g_{NL} \end{bmatrix}_{[G_{LT}]_{K \times L}} \cdot \begin{bmatrix} C[0] \\ \vdots \\ C[L-1] \end{bmatrix}_{[C]_{L \times 1}} \quad (4)$$

Декодування вихідних символів відбувається безпосередньо із відповідних прийнятих закодованих символів з власним ідентифікатором закодованого символу. Декодування відсутніх вихідних символів відбувається із відновлених проміжних символів C відповідно до виразу (4). Щоб отримати C із формули (3), стандартний алгоритм декодування передбачає, що підматриця $[A]_{M \times L}$ має повний ранг стовпця [13, 14].

Слід зазначити, що всі вихідні символи не можуть бути відновлені, навіть якщо ($N' \geq K$). За умови, що ($N' < K$), декодер також не може декодувати всі проміжні і вихідні символи, він відновлює вихідні символи із відповідних прийнятих закодованих символів з відповідним ідентифікатором.

Алгоритм стандартного процесу декодування коду Шокролахі, описаний в [15], використовує метод Гауса і алгоритм поширення довіри для перетворення матриці A в одиничну матрицю розміром $L \times L$ після відкидання останніх рядків $M - L$, так як ефективність обчислень методом Гауса залежить від розрідженості матриці A , то для підтримки її розрідженості використовується алгоритм поширення довіри. Процес перетворення матриці A в одиничну матрицю складається з чотирьох етапів, рис. 1 – 4 [15].

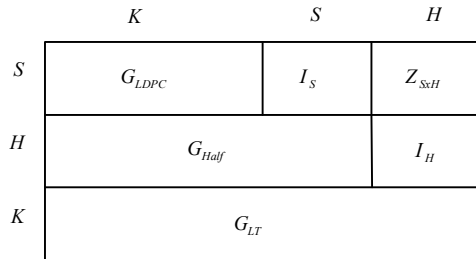


Рис 1. Матриця A

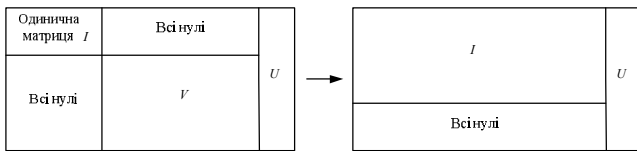


Рис 2. Підматриця матриці A .
Перший етап перетворення в одиничну матрицю I

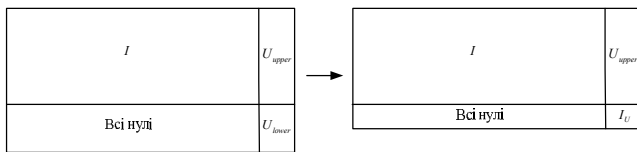


Рис 3. Другий етап перетворення матриці A в одиничну матрицю I

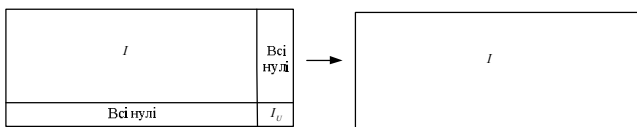


Рис 4. Третій і четвертий етапи перетворення матриці A в одиничну матрицю I

На першому етапі матриця A перетворюється в три підматриці: I , нульову підматрицю та U . На початку першої фази $V = A$, де V – проміжна матриця, а підматриці I та U є нульовими матрицями. При кожній ітерації вибирається рядок із матриці V з мінімальним ненульовим ступенем r . Потім обраний рядок обмінюється місцями із першим рядком в матриці V . Всі стовпчики V переставляються так, щоб перший і останній $r - 1$ елементи першого рядка були одиницями. Потім над рештою рядків, в першому стовпці яких є одиниці, проводиться операція «XOR» з першим рядком, в результаті чого стовпці стають нульовими.

При цьому ранг підматриці I збільшується на одиницю, а число стовпців в матриці U збільшується на $r - 1$. Цей процес повторюється доти, поки сума стовпців I і U не стане дорівнювати L . Пе-

рший етап може припинитися через виникнення збою, якщо в V не залишається жодного ненульового рядка до моменту виродження V , тобто сума стовпців I та U буде менше за L , а елементи у всіх рядках V дорівнювати нулю.

На другому етапі підматриця U розбивається на U_{upper} і U_{lower} , при цьому U_{upper} складається із перших i рядків, U_{lower} містить останні рядки $M - i$. Якщо ранг U_{lower} менше ніж u , виникає збій, другий етап процесу декодування припиняється. В іншому випадку U_{lower} трансформується в одиничну матрицю із рангом u , а останні $M - L$ рядки з $[A]_{M \times L}$ відкидаються.

На третьому етапі процесу декодування на основі матриці I_U генерується матриця U' .

На четвертому етапі для обнуління матриці U_{upper} використовується матриця U' , та відбувається повне перетворення матриці A в одиничну матрицю розміром $L \times L$.

Успішне завершення процесу декодування залежить від процесу перетворення матриці A в одиничну матрицю розміром $L \times L$. Проміжні символи S можуть бути декодовані на основі операцій з рядками й обміні рядків та стовпців.

На рис. 5 наведено приклад застосування алгоритму поширення довіри і методу Гауса для трансформації матриці A в одиничну матрицю.

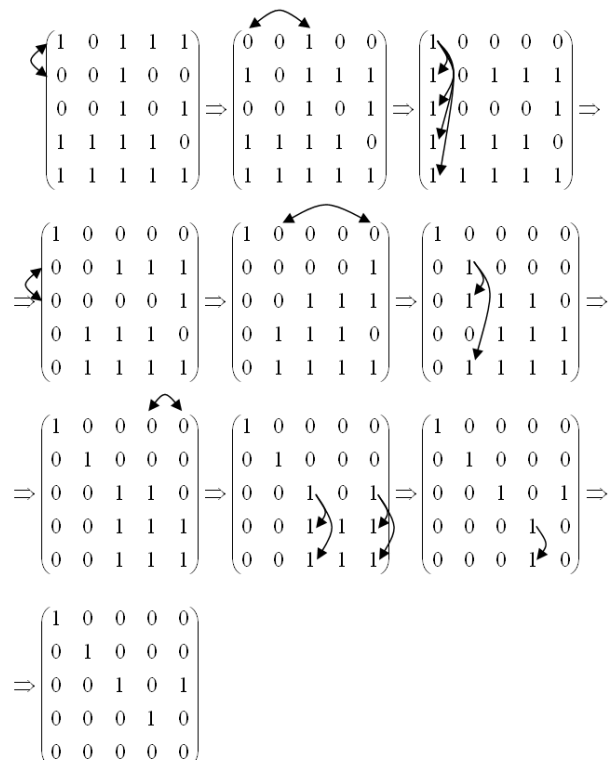


Рис 5. Приклад використання алгоритму поширення довіри і методу Гауса для трансформації матриці A

Стрілочками позначається обмін стовпців та строк. При застосуванні алгоритму поширення довіри і методу Гауса індекси стовпців, які беруть участь в перестановці, зберігаються. На останній

матриці видно, що при декодуванні на другому етапі виник збій, оскільки ранг U_{lower} , де U_{lower} є останнім рядком підматриці U в цьому прикладі, дорівнює 0, що менше числа стовпців в U ($u = 1$).

2. Удосконалений алгоритм для прискореного декодування коду Шокролахі.

Удосконалений алгоритм дозволяє значно скоротити час обчислень на першому і другому етапах декодування, в порівнянні з алгоритмом, що описано в [15]. Удосконалений алгоритм включає в себе процедуру відтворення декодування з моменту виникнення збою на першому або другому етапах.

Стандартний процес декодування [15] може припинитися через збій, що виникає на першому етапі, якщо в підматриці V всі рядки стали нульовими до того, як підматриця V виродилася, і на другому етапі, якщо ранг матриці U_{lower} менше ніж u . Якщо процес декодування припиняється через збій на перших двох етапах, декодеру необхідно отримати достатньо нових закодованих символів, щоб запустити декодування з початку.

При використанні процедури відтворення декодування з моменту виникнення збою зберігаються індекси стовпців, які беруть участь в перестановках, що відбуваються при застосуванні методу Гауса для перетворення U_{lower} в одиничну матрицю з рангом u . Коли i -й та i' -й стовпці матриці A обмінюються місцями, відбувається запис пари їх індексів. Якщо декодування припиняється через збій на першому або другому етапах, то n додатково отриманих закодованих символів додаються в D у виразі (3), а n нових рядків породжувальної матриці $[G_{LT}]_{n \times L}$ додаються в нижню частину матриці A .

По останній матриці на рисунку 5 видно, що виник збій при декодуванні. Відповідно запропонованого алгоритму стовпці, засновані на записаних індексах для підматриці $[G_{LT}]_{n \times L}$, повинні обмінятися місцями. Після цього між кожним рядком оновленої підматриці $[G_{LT}]_{n \times L}$ і кожним рядком одиничної підматриці I в матриці A проводиться операція «XOR». За рахунок даної процедури досягаються результати, аналогічні результатам при застосуванні алгоритму поширення довіри та методу Гауса, але декодування не переривається та не починає працювати з самого початку, а декодувальний процес продовжується. Далі застосовуються метод Гауса та алгоритм поширення довіри, які трансформують оновлену матрицю A в одиничну матрицю, починаючи з моменту виникнення збою в процесі декодування.

Через те, що при декодуванні виник збій, до матриці додається новий рядок на основі значення ідентифікатора закодованого символу. Згідно алгоритму нової запропонованої процедури стовпці нового доданого рядка обмінюються місцями на основі індексів записаних стовпців, наведених на рисунку 5. Після цього проходить операція «XOR» з рядками одиничної матриці I та отриманим новим рядком, щоб виключити одиницю з нового рядка від 0 до

($i-1$). В результаті даних операцій отримуємо остаточною одиничну матрицю.

У коді Шокролахі ймовірність збою $P_e(\cdot)$ при декодуванні вихідного блоку, тобто ймовірність того, що щонайменше один вихідний символ у вихідному блоці не відновиться, може бути обчислена [16] виразом (5).

$$P_e(K) = \begin{cases} 1 & \text{if } \varepsilon(K) < 0 \\ 0.85 \times 0.567^{\varepsilon(K)} & \text{if } \varepsilon(K) \geq 0 \end{cases} \quad (5)$$

Середнє число додаткових (надлишкових) даних $\bar{R}_e(K)$, необхідних для успішного декодування після кожного виникнення збою обчислюється за формулою (6) [16]:

$$\begin{aligned} \bar{R}_e(K) &= \frac{1}{K} \sum_{i=0}^{\infty} i \cdot (P_e(i-1) - P_e(i)) = \\ &= \frac{0.85}{K} \sum_{i=0}^{\infty} i \cdot (0.567^{i-1} - 0.567^i) = \\ &= \frac{0.85}{(1-0.567)K} \approx \frac{2}{K} \end{aligned} \quad (6)$$

Як видно із (6), середня кількість додаткових закодованих символів, необхідних для вихідного блоку з розміром K , $K \times 2 / K = 2$, тобто не залежить від K . З цієї причини, коли $N' \geq K$ і процес декодування припиняється через виникнення збою, запропонований алгоритм продовжує декодування після прийому $n = 2$ додаткових закодованих символів.

У розглянутому алгоритмі коду Шокролахі [15] процес декодування не може розпочатися до тих пір, поки не будуть отримані як мінімум N' закодованих символів ($N' \geq K$). У запропонованому алгоритмі відтворення декодування з моменту виникнення збою декодування починається при $N' < K$, при цьому декодер продовжує отримувати додаткові закодовані символи до тих пір, поки $N' \geq K$. Дана процедура значно скорочує час процесу декодування вихідних символів.

3. Експериментальні результати.

У статті наведені результати обчислень часу декодування коду Шокролахі, досягнуті запропонованим та стандартним алгоритмами.

Запропонований удосконалений алгоритм декодування відрізняється від стандартного алгоритму процедурою першого і другого етапів. Ця відмінність дає вигоду у часі, який у стандартному алгоритмі витрачається на операції декодування проміжних символів.

Виконання першого та другого етапів займають більше 90% від загального часу декодування, тому вкрай важливо мати можливість не розпочинати декодування з початку першого етапу при виникненні збою, щоб скоротити загальний час обчислень при декодуванні коду Шокролахі.

На рис. 6 – 7 наведено час, витрачений на декодування коду Шокролахі при використанні стандартного алгоритму декодування [15] і запропонованої процедури відтворення декодування з моменту виникнення збою за умови, що збій декодування коду Шокролахі відбувається на першому етапі процесу перетворення матриці A .

На рис. 6 приведена продуктивність алгоритмів за умови, що розмір вихідних символів l фіксований і дорівнює 256 байтів, а кількість вихідних символів K змінюється до 2000. На рис. 7 приведена продуктивність алгоритмів при фіксованій кількості вихідних символів 1024 на блок, та змінному розмірі символів.

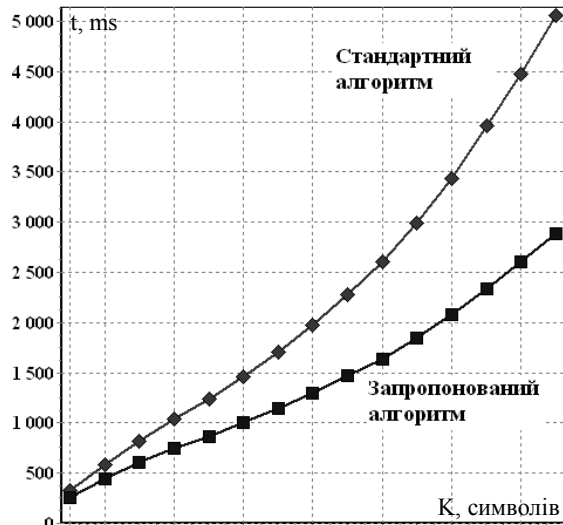


Рис. 6. Час декодування зі збоєм на першому етапі стандартним і запропонованим алгоритмами при розмірі символу 256 байт

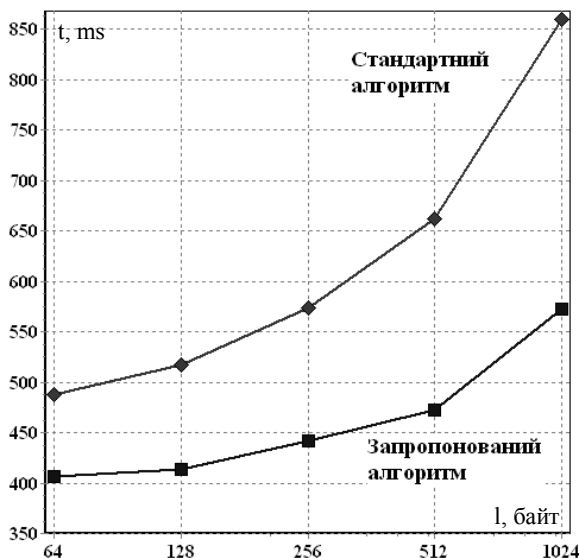


Рис. 7. Час декодування зі збоєм на першому етапі стандартним і запропонованим алгоритмами при кількості символів у блоці 1024

При використанні запропонованої процедури відтворення декодування з моменту виникнення збою досягається виграш у часі декодування в 1,3 –

1,7 разів, в порівнянні із застосуванням стандартного алгоритму. Це пов'язано з тим, що пропонується процедура продовжує декодування після прийому додаткових символів без перезапуску з першого етапу.

На рис. 8 – 9 наведено час, витрачений на декодування коду Шокролахі при виникненні збою на другому етапі. При застосуванні стандартного алгоритму, коли процес декодування завершується виникненням збою на другому етапі, обидва етапи, перший і другий, повторюються спочатку.

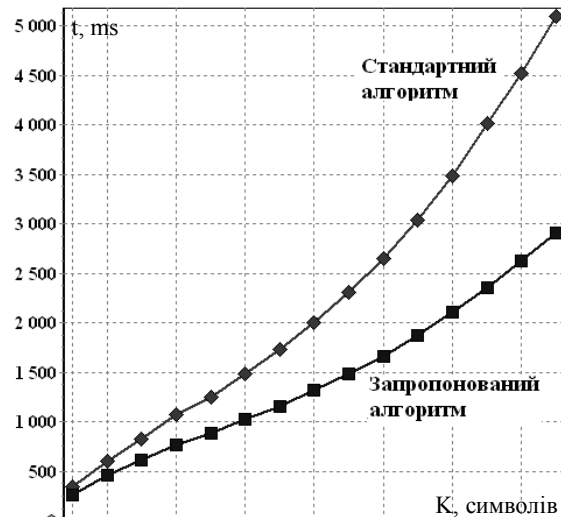


Рис. 8. Час декодування зі збоєм на другому етапі при розмірі символу 256 байт

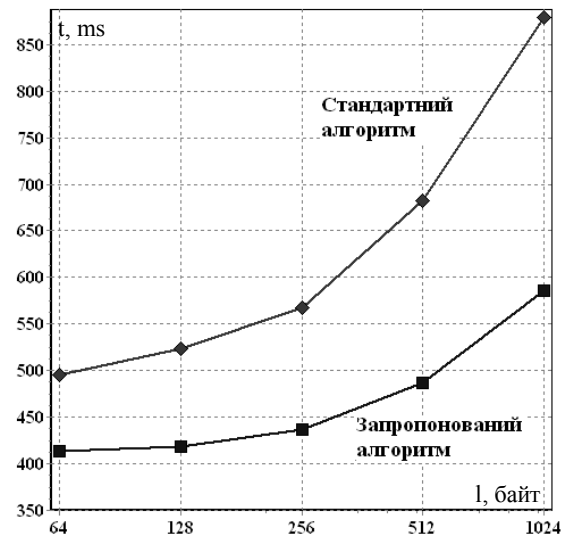


Рис. 9. Час декодування зі збоєм на другому етапі при кількості символів у блоці 1024

Висновки

В даній статті запропоновано використання вдосконаленої процедури декодування мультимедіа даних, закодованих одним із завадостійких фонтанних кодів – кодом Шокролахі. Застосування даної процедури дає можливість підвищити достовірність та оперативність передачі мультимедіа даних. Удосконалення процесу декодування полягає в тому, що

при виникненні збою декодування продовжує свою роботу з моменту виникнення збою, не повертаючись до початку першого етапу, як це відбувається при роботі стандартного алгоритму Шокролахі. Застосування даної процедури дозволяє отримати виграш у часі декодування мультимедійної інформації від 1,3 до 1,7 разів в залежності від кількості переданих символів у блоках інформації і розміру пере-

даних символів у відповідних блоках. У статті наведено результати порівняльного аналізу роботи запропонованого алгоритму і стандартного алгоритму декодування, які доводять ефективність застосування удосконаленого підходу при передачі мультимедіа даних для підвищення таких характеристик якості обслуговування, як достовірність і оперативність.

СПИСОК ЛІТЕРАТУРИ

1. Eur-lex: green paper on a european programme for critical infrastructure protection [Електронний ресурс]. – Brussels, 2005. – Режим доступу: http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf.
2. Eur-lex: communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection [Електронний ресурс]. – Brussels, 2006. – Режим доступу: http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf.
3. European Commission: a Communication on Protecting Europe's Critical Energy and Transport Infrastructure [Електронний ресурс]. – Brussels, 2007. – Режим доступу: <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%206315%202007%20EXT%201%20REV%201>.
4. Eur-lex: council directive 2008/114/EC of 8 December on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [Електронний ресурс]. – Brussels, 2008. – Режим доступу: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF>.
5. Зелена книга з питань захисту критичної інфраструктури в Україні / Д. С. Бірюков, С. І. Кондратов, О. І. Насвіт, О. М. Суходоля. – Київ : Національний інститут стратегічних досліджень, 2015. –30 с.
6. Верховна Рада України: наказ про затвердження Положення про систему управління безпекою руху поїздів у Державній адміністрації залізничного транспорту України [Електронний ресурс] / Міністерство Інфраструктури України, 2011. – Режим доступу до наказу: <http://zakon3.rada.gov.ua/laws/show/z0729-11>.
7. Верховна Рада України: постанова про затвердження Державної цільової програми реформування залізничного транспорту на 2010-2019 роки [Електронний ресурс] / Кабінет Міністрів України, 2009. – Режим доступу до постанови: <http://zakon3.rada.gov.ua/laws/show/1390-2009-%D0%BF>.
8. Васильев В. М. Анализ методов передачи видеоинформации в компьютерных сетях / В. М. Васильев, Ю. В. Гугель, И. П. Гуров // Научно-технический вестник информационных технологий, механики и оптики. – 2002. – С. 14-26.
9. Tirlitti T. Videoconferencing on the internet / T. Tirlitti, C. Huitema // IEEE/ACM Trans. Netw. Vol. 4. – 1996. – P. 340-351.
10. Wu D. Transporting real-time video over the internet: challenges and approaches / D. Wu, Y. T. Hou, Y. Zhang // IEEE proc. V. 88. – 2000. – P. 1855-1875.
11. Why Digital Fountain's Raptor Technology Is Better Than Reed-Solomon Erasure Codes For Streaming Applications // Digital Fountain. – 2010. – P. 6-8.
12. Toit J. A Practical Implementation of Fountain Codes over WiMAX Networks with an Optimized Probabilistic Degree Distribution / J. Toit, R. Wolhuter // The Sixth International Conference on Systems and Networks Communications. – 2011. – P. 32-37.
13. Shokrollahi A. Raptor codes / A. Shokrollahi // Transactions on information theory. – 2006. – P. 2551-2567.
14. Shokrollahi A. Raptor codes – foundations and trends in communications and information theory / A. Shokrollahi, M. Luby // Foundations and Trends in Comm. and Inf. Theory. – 2011. – P. 213-322.
15. 3GPP. 3GPP TS 26346 V741: Technical Spec Group Serv and Sys Aspects; Multimedia Broadcast/Multicast Service (MBMS); Protocols and Codecs. 3GPP TechnicalSpec. – 2007. – P. 156-161.
16. Application layer forward error correction for mobile multimedia broadcasting / T. Stockhammer, A. Shokrollahi, M. Watso, M. Luby, T. Gasiba // Handbook of Mobile Broadcasting. – 2008. – P. 239-280.

REFERENCES

1. Eur-lex : green paper on a european programme for critical infrastructure protection (2005), Brussels, available at: http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf (last accessed January 29, 2018).
2. Eur-lex : communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection (2006), Brussels, available at: http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf (last accessed January 29, 2018).
3. European Commission : a Communication on Protecting Europe's Critical Energy and Transport Infrastructure (2007), Brussels, available at: <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%206315%202007%20EXT%201%20REV%201> (last accessed January 29, 2018).
4. Eur-lex : council directive 2008/114/EC of 8 December on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (2008), Brussels, available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF> (last accessed January 29, 2018).
5. Biryukov, D.S., Kondratov, S.I., Nasvit, O.I. and Sukhodolya, O.M. (2015), *Green Paper on the Protection of Critical Infrastructure in Ukraine*, National Institute for Strategic Studies, Kyiv, 30 p.
6. Verkhovna Rada of Ukraine: an order to approve the Regulation on the system of safety management of trains in the State Administration of Railway Transport of Ukraine, available at: <http://zakon3.rada.gov.ua/laws/show/z0729-11> (last accessed January 29, 2018).

7. Verkhovna Rada of Ukraine: Resolution on Approval of the State Target Program for the Reform of Rail Transport for 2010-2019, available at: <http://zakon3.rada.gov.ua/laws/show/1390-2009-%D0%BF> (last accessed January 29, 2018).
8. Vasiliev, V.M., Gugel, Yu.V. and Gurov, IP (2002), "Analysis of methods for the transmission of video information in computer networks", *Scientific and Technical Bulletin of Information Technologies, Mechanics and Optics*, pp. 14-26.
9. Tirletti, T. and Huitema C. (1996), "Videoconferencing on the internet", *IEEE/ACM Trans. Netw.*, Vol. 4, pp. 340-351.
10. Wu, D., Hou, Y.T. and Zhang, Y. (2000), "Transporting real-time video over the internet: challenges and approaches", *IEEE Proc.*, Vol. 88, pp. 1855-1875.
11. Why Digital Fountain's Raptor Technology Is Better Than Reed-Solomon Erasure Codes For Streaming Applications (2008), *Digital Fountain*, pp. 6-8.
12. Toit, J. and Wolhuter, R. (2011), "A Practical Implementation of Fountain Codes over WiMAX Networks with an Optimized Probabilistic Degree Distribution", *The 6th International Conference on Systems and Networks Communications*, pp. 32-37.
13. Shokrollahi, A. (2006), "Raptor codes", *Transactions on information theory*, pp. 2551-2567.
14. Shokrollahi, A. and Luby M. (2001), "Raptor codes – foundations and trends in communications and information theory", *Foundations and Trends in Comm. and Inf. Theory*, pp. 213-322.
15. 3GPP. 3GPP TS 26346 V741: Technical Spec Group Serv and Sys Aspects; Multimedia Broadcast/Multicast Service (MBMS); Protocols and Codecs (2007), *3GPP TechnicalSpec*, pp. 156-161.
16. Stockhammer, T., Shokrollahi, A., Watso, M., Luby, M. and Gasiba T. (2008), "Application layer forward error correction for mobile multimedia broadcasting", *Handbook of Mobile Broadcasting*, pp. 239-280.

Надійшла (received) 28.02.2018

Прийнята до друку (accepted for publication) 18.04.2018

Усовершенствование процесса декодирования мультимедиа данных, закодированных алгоритмом Шокролахи

С. Г. Семенов, О. В. Липчанская, М. В. Липчанский

Предметом изучения в статье являются процессы передачи данных в системах критического применения. Целью является разработка усовершенствованного алгоритма декодирования мультимедиа данных, закодированных помехоустойчивым фонтанным кодом Шокролахи. Задачи: повысить достоверность и оперативность декодирования мультимедиа данных, передаваемых по беспроводным каналам связи, рассмотреть существующие алгоритмы кодирования и декодирования Шокролахи для передачи мультимедиа данных по каналам со стираниями, адаптировать существующий код к повышенным требованиям оперативности и достоверности путем усовершенствования процедуры декодирования видеoinформации, провести сравнительный анализ эффективности работы предложенной процедуры по отношению к существующей стандартной процедуре. Используемыми методами являются: помехоустойчивый фонтанный код Шокролахи, метод Гаусса, алгоритм распространения доверия, LT код. Получены следующие результаты: сформулирована задача повышения достоверности и оперативности декодирования мультимедиа данных, усовершенствована процедура декодирования мультимедиа данных, закодированных фонтанным кодом Шокролахи, на примере сравнительного анализа показана эффективность работы данной процедуры по сравнению с существующим алгоритмом декодирования. Выводы: научная новизна полученных результатов состоит в следующем: усовершенствована стандартная процедура декодирования Шокролахи путем организации возможности продолжать декодирование при возникновении сбоя с момента сбоя, не возвращаясь к началу первого этапа. Выигрыш во времени составляет от 1,3 до 1,7 раз в зависимости от размера передаваемых символов и количества символов в кодируемых блоках. Полученный результат является важным в силу того, что время является одной из основных характеристик показателей качества передачи данных.

Ключевые слова: фонтанные коды, коды Шокролахи, декодирование мультимедиа данных, системы критического применения, оперативность и достоверность передачи данных.

Improvement of the decoding process for multimedia data encoded by the Shokrollahi algorithm

S. Semenov, O. Lipchanska, M. Lipchanskyi

The subject of the study in the article are the processes of data transmission in mission-critical systems. The goal is to develop an improved algorithm for decoding multimedia data encoded with a fountain code of Shokrollahi. The tasks to be solve are to increase the reliability and efficiency of decoding multimedia data transmitted over wireless communication channels, to consider the existing algorithms for Shockollachi encoding and decoding for transferring multimedia data through channels with erasures, to adapt the existing code to increased demands for efficiency and reliability by improving the procedure for decoding video information, to perform a comparative analysis effectiveness of the proposed procedure in relation to the existing standard procedures . The methods used are: error correction and detection fountain code of Shokrollahi, Gauss method, confidence distribution algorithm, LT code. The following results were obtained: the task of increasing the reliability and efficiency of decoding multimedia data was formulated, the procedure for decoding multimedia data encoded with the Shokrollahi fountain code was improved. The efficiency of the procedure compared with the existing decoding algorithm is shown using the example of a comparative analysis. Conclusions: the scientific novelty of the results obtained is as follows: the standard procedure for decoding Shockollachi has been improved by organizing the possibility of continuing decoding in case of a failure from the moment of failure, without returning to the beginning of the first stage. The time gain is 1.3 to 1.7 times, depending on the size of the transmitted symbols and the number of symbols in the coded blocks. The obtained result is important because time is one of the main characteristics of data transmission quality parameters.

Keywords: fountain codes, Shockollachi codes, decoding of multimedia data, mission-critical systems, efficiency and reliability of data transmission.