УДК 004.056

Фауре Е.В., Харін О.О.
Черкаський державний технологічний університет

Дослідження ймовірності виникнення помилки декодування під час використання факторіального коду з відновленням даних

Факторіальним кодом з відновленням даних по перестановці (ФКВД) називається несистематичний код, в якому носієм інформаційної послідовності з k біт є перестановка чисел порядку M, що обирається з умови $M! \geq 2^k$, обчислена по всім бітам вхідної послідовності. ФКВД забезпечує криптографічний захист та захист від помилок в каналі зв'язку, а також має здатність до самосинхронізації і не потребує маркера для розділення блоків під час сеансу зв'язку.

Метою роботи є дослідження за допомогою розрахунково-експериментального методу ймовірності не виявленої ФКВД помилки під час передавання повідомлення каналом зв'язку з незалежними бітовими помилками.

У відповідності до [1, 2], математична модель ймовірності не виявленої ФКВД помилки

$$P_{ud}\left(FCDR, p_0\right) \leq \sum_{i=1}^{m_1} f_{per}\left(2i\right) p_0^{2i} q_0^{r-2i} + \Delta_{per}\left(m_1\right), \qquad (1)$$

де $f_{per}\left(0\right)=1;\ f_{per}\left(2\right) \leq l_r \cdot M/2;\ f_{per}\left(4\right) \leq l_r \cdot M \cdot \left(l_r \cdot \left(M+8\right)-10\right)/8;$

$\Delta_{per}\left(m_1\right) \leq e^{-\lambda} \cdot \frac{\lambda^{2\left(m_1+1\right)}}{\left(2\left(m_1+1\right)\right)!} \times \frac{\left(2m_1+3\right)^2}{\left(2m_1+3\right)^2-\lambda^2};$ $\quad l_r = \text{entier}\left(\log_2 M\right)+1,$ функція

$\text{entier}\left(a\right)$ визначає найбільше ціле, менше за a; $r = l_r \cdot M$; $\lambda = r \cdot p_0$;

m_1 обирається таким чином, щоб $m_1 > \left(\lambda-3\right)/2$ і оцінка $\Delta_{per}\left(m_1\right)$ не перевищувала заданої максимальної похибки обчислень.

Для знаходження точних значень абсолютних частот $f_{per}\left(i\right)$ у залежності від параметрів кодування розроблено імітаційну модель, що передбачає наступні дії:

1) для кожного інформаційного вектору $A\left(x\right)$, що складається з k інформаційних біт $\left(A\left(x\right) \in \left[0; 2^k-1\right]\right)$, формується перестановка π порядку M. Під час цього перетворення $M! \geq 2^k$, а $\left(M!-2^k\right)$ перестановок є забороненими;

2) перестановка π після кодування її символів рівномірним двійковим кодом перетворюється в r-розрядну двійкову послідовність $R_{FCDR}\left(x\right)$ $\left(R_{FCDR}\left(x\right) \in \left[0; 2^r-1\right]\right)$;

3) на сформовану послідовність $R_{FCDR}\left(x\right)$ по черзі накладаються r-розрядні вектори помилки $\varepsilon\left(x\right) \in \left[0; 2^r-1\right]$. У залежності від вектору помилки $\varepsilon\left(x\right)$ можливі наступні варіанти модифікації представленої в двійковому вигляді перестановки π:

- трансформація перестановки в перестановку:
  - a) з дозволеної множини,
  - b) з забороненої множини;
- трансформація перестановки в не перестановку;

4) виконується підрахунок абсолютних частот $f_{per}\left(i\right)$

трансформації перестановки π в перестановку π' з дозволеної множини у залежності від ваги Хеммінга *i* вектору помилки $\varepsilon(x)$.

Для скорочення кількості операцій під час експериментального обчислення значень $f_{per}(i)$ виконано заміну операції $R'_{FCDR}(x) = R_{FCDR}(x) \oplus \varepsilon(x)$ на операцію $\varepsilon(x) = R_{FCDR}(x) \oplus R'_{FCDR}(x)$, де $R'_{FCDR}(x)$ приймає всі можливі двійкові комбінації, що відповідають перестановкам дозволеної та забороненої множин.

У результаті проведення експерименту отримано наступні результати:

1) оскільки потужність множини векторів помилки $\varepsilon(x)$ більша за потужність множини перестановок порядку M $\left(2^r > M!\right)$, то кількість векторів помилок, які призводять до трансформації перестановки в не перестановку, дорівнює $2^r - M!$;

2) оскільки порядок перестановки M обирається з умови $(M-1)! \le 2^k \le M!$, то частина перестановок відноситься до забороненої множини для забезпечення рівної потужності множини значень інформаційних векторів і множини дозволених перестановок. У такому випадку кількість векторів помилок, які призводять до трансформація перестановки в перестановку із забороненої множини, дорівнює $M! - 2^k$;

3) оскільки множина всіх можливих інформаційних векторів дорівнює 2^k, то кількість векторів помилок, що призводять до трансформація перестановки в іншу дозволену перестановку, включаючи саму себе, також дорівнює 2^k;

4) отримані співвідношення кожного з типів помилок до загальної потужності множини векторів помилок не залежать від розміру і вмісту інформаційної послідовності.

Враховуючи особливості ФКВД, помилки, що призводять до трансформації перестановки в не перестановку або до трансформації перестановки в заборонену перестановку, виявляються кодом і не призводять до помилкового декодування даних. Помилкове декодування можливе лише у випадку, коли під впливом вектору помилки перестановка π перетворюється в перестановку π', яка входить до множини дозволених перестановок.

У результаті експерименту підтверджено, що до трансформації перестановки в перестановку призводять тільки вектори помилок с вагою Хеммінга, кратною 2. Накопичена статистика дозволяє уточнити значення $f_{per}(i)$ і, як наслідок, імовірність не виявленої ФКВД помилки $P_{ud}(FCDR, p_0)$. Встановлено, що ФКВД виявляє більш ніж 99.5% помилок і цей показник зростає зі збільшенням порядку перестановки M (при M = 7 відсоток невиявлених помилок становить 0.195%, в той час коли для M = 10 – 0.00019%) за рахунок зростаючої збитковості, що в свою чергу призводить до зниження швидкості коду. Оптимальним є вибір такого розміру інформаційного блоку, при якому $k = entier(\log_2 M!)$.

Список використаних джерел

1. *Фауре Э.В. Факториальное кодирование с восстановлением данных / Э.В. Фауре // Вісник Черкаського державного технологічного університету. – 2016. – №2. – С. 33-39.*
2. *Фауре Э.В. Контроль целостности информации на основе факториальной системы счисления / Э.В. Фауре, В.В. Швыдкий, А.И. Щерба // Journal of Qafqaz University. Mathematics and computer science. – 2016.*