

Завадостійке перетворення інформації

К.т.н., доц. О. Різник, асист. Д. Скрибайло-Леськів

Lviv Polytechnic National University, 22/806 Bandera St., Lviv-13, 79013, Ukraine

Abstract. Advantage of the offered method of construction of nonuniform code sequences on the basis of ideal circular bundles is to the high antijamming code, both from an unauthorized division and from distortion of information

Key words: idea ring bundle, cyclic redundancy code, Hamming code, monolithic code.

Завадостійке кодування перетворення інформації займає важливе місце в сучасних системах передачі даних, зв'язку. На сьогоднішній день існує велика кількість способів завадостійкого кодування, які активно використовуються в різних системах передачі даних і, отже, зберігають актуальність дослідження.

Головною проблемою сучасної теорії і техніки зв'язку є підвищення завадозахищеності систем телекомунікацій і, особливо, в умовах впливу як природних завад, так і створюваних штучних завад. Одна з основних концепцій підвищення завадозахищеності, що розробляється в магістерській роботі, полягає в тому, щоб оперативно проводити зміну робочих ансамблів кодів, збільшуючи тим самим завадостійкість, а також захист інформації від несанкціонованого доступу.

Метою є дослідження одного з методів завадостійкого перетворення інформації, заснованого на використанні двійкових кодових комбінацій, а саме, двійкових циклічних нееквідистантних кодів.

Розроблений метод спрощеного синтезу завадостійкої багатопозиційної кодової послідовності на основі числових в'язанок та створення ефективного алгоритму кодування і декодування інформації. Дослідження показують, що використання багато-позиційних кодових послідовностей на основі числових в'язанок в задачах перетворення інформації забезпечує більшу ефективність у порівнянні з кодами БЧХ.

Дослідження різних типів багатопозиційних кодів свідчить про переваги тих із них, які синтезовані на основі числових в'язанок, що дає змогу досягнути більшої завадостійкості при перетворенні інформації в порівнянні з класичними багатопозиційними кодовими послідовностями [1].

Завадостійке кодування дозволяє підвищити вірність передавання повідомлень. Це обумовило широке використання кодів у сучасних системах передачі інформації. Можливість виявляти і виправляти помилки в прийнятих повідомленнях з'являється за рахунок введення надлишковості при кодуванні на передаючому боці.

Джерело повідомлень виробляє будь-які повідомлення, але після кодеру джерела, у більшості систем передачі інформації, ці повідомлення мають вигляд безперервного двійкового повідомлення. Прийнято вважати, що символи в послідовності на виході кодеру джерела мають випадковий характер та не залежать один від одного.

Основна задача систем передачі інформації – передавання інформації з фіксованими вірністю та швидкістю. Ці вимоги суперечні, і підвищення швидкості призводить до зниження завадостійкості передачі. Проте безпомилкова передача інформації є можливою, якщо продуктивність джерела не перевищує пропускної здатності каналу. Досягається це використанням досить довгих коригуючих кодів. На практиці довжина кодів обмежена допустимою складністю приладів кодування та декодування. Задача відшукування кодів складається в забезпеченні необхідної вірогідності передачі при кінцевій довжині і припустимій надлишковості.

В даній роботі реалізоване завадостійке перетворення інформації на основі багатопозиційних кодів на основі числових в'язанок. Поставленою метою є використання числових в'язанок для кодування інформації (текстової, графічної, аудіо, відео та іншої), яка міститься у вхідному файлі. Закодований файл може бути переданий по мережі на інший комп'ютер. На цьому комп'ютері закодований файл повинен бути розкодований зворотнім методом і повинен містити таку ж інформацію, яка була у вхідному файлі.

В основі методу кодування за допомогою числових в'язанок лежить принцип представлення коду кожного символу у вигляді масиву, що складається з нулів і одиниць. Це кодування подібне до перетворення в двійкову систему числення, але, в випадку кодування числовими в'язанками, відстань між однойменними розрядами рівна відповідному числу з цієї в'язанки.

Ідеальною кільцевою в'язанкою N -порядку називається послідовність $K_n=(k_1, k_2, \dots, k_i, \dots, k_N)$ чисел, на якій всі можливі кільцеві суми вичерпують R -разів значення чисел натурального ряду $1, 2, \dots, S_N$, де $S_N=N(N-1)/R+1$.

Розглянемо кодову послідовність, якому присвоєні ваги ІКВ 8-го ($N=8$) порядку кратності ($R=4$): $1, 1, 1, 2, 2, 1, 3, 4$. Оскільки значення ваг — це числа ІКВ 8-го порядку 4-ої кратності, кожне число натурального ряду від 1 до $n(n-1)/r+1=15$ можна отримати чотирьома способами, а число всіх способів дорівнює кількості одержаних чисел.

При заданій кількості n розрядів кодової послідовності система дає змогу кодувати будь-які числа від 1 до $S_n=n(n-1)/r+1$.

Кодові комбінації 10000000, 01000000, 00100000, 00000100 відповідають 4-м варіанта представлення числа 1. Кодуванню числа 2 відповідають 11000000, 01100000, 00010000, 00001000. Числу 3 відповідають 11100000, 00110000, 00001100, 00000010, числу 4 — 01110000, 00011000, 00000110, 00000001 і т. д., числу 14 — 01111111, 10111111, 11011111, 11111011, числу 15 — 11111111.

Кожній числовій комбінації кодової послідовності відповідає набір пакетів одиниць та нулів, який будується згідно ваг ІКВ за наступним правилом:

1 це 1, 2 – 10, 3 – 100, 4 – 1000 і так далі.

Кількість різних $S_N(S_N-1)/2$ кодових комбінацій містить точно R із N одиничних символів в однойменних розрядах, що впливає з властивостей ІКВ.

Решта N-R символів однієї і стільки ж іншої кодової послідовності на основі ІКВ відрізняються від символів, що містяться в однойменних розрядах.

Тому мінімальна кодова відстань для будь-якої кодової послідовності на основі ІКВ визначається як наступне співвідношення порядку та кратності ІКВ:

$$d_{\min} = 2(N-R)$$

Для збільшення потужності кодової послідовності на основі ІКВ побудуємо дзеркальну кодову послідовність з вагами ІКВ, де поміняємо місцями одиниці і нулі при кодуванні.

Кодові комбінації 01111111, 10111111, 11011111, 11110111 відповідають 4-м варіантам представлення числа 1. Кодуванню числа 2 відповідають 00111111, 10011111, 11011111, 11110111. Числу 3 відповідають 00011111, 11001111, 11110011, 11111101, числу 4 — 10001111, 11100111, 11111001, 11111110 і т. д., числу 14 — 10000000, 01000000, 00100000, 00000100, числу 15 — 00000000.

Кожна з різних пар кодових комбінацій зустрічається точно R-разів із N одиничних символів в однойменних розрядах. Мінімальна кодова відстань для даного коду визначається як:

$$d_{\min} = 2 \times (N - R)$$

Число помилок t_d , які можна виявити, та число помилок t_c , що можна виправити за допомогою коригувального коду, зв'язані з мінімальною кодовою відстанню d_{\min} залежностями:

$$t_d \leq d_{\min} - 1$$

$$t_c \leq \frac{d_{\min} - 1}{2}$$

Задача зводиться до забезпечення найбільшої мінімальної кодової відстані d_{\min} при якомога меншому значенні S_N .

Побудову таблиці дозволених кодових комбінацій можна розбити на наступні етапи:

- виділити рядок із S_N пронумерованих у зростаючому порядку кліток одновимірного масиву
- заповнити інформаційними «одиницями» клітки, номери яких збігаються з числами, визначеними з ІКВ за формулою:

$$x_j - 1 \equiv \sum_{i=1}^j k_i \pmod{S_N}, j = 1, 2, \dots, n$$

- занести «нулі» у клітки, що залишилися незаповненими.

Проведемо порівняння завадостійкого коду на ідеальних кільцевих в'язанках з різними параметрами N та R.

Параметри в'язанки	N=8, R=4	N=15, R=7	N=6, R=1	N=32, R=16
Мінімальна кодова відстань	8	16	10	32
Кількість виявлених помилок	7/47%	15/48%	9/29%	31/49%
Кількість виправлених помилок	3/20%	7/23%	4/13%	15/24
Довжина вхідного блоку в бітах	4	5	5	6
Довжина вихідного блоку в бітах	15	31	31	63
Надлишковість в бітах	11	26	26	57
Розмір до кодування (байт)	2018077	2018077	2018077	2018077
Розмір після кодування (байт)	8072308	12915696	12915696	21526160
Співвідношення	4	6,4	6,4	10,67

При порівнянні завадостійкого кодування на ІКВ та БЧХ перетворення інформації на основі кодів БЧХ показує вищу коригувальну здатність при меншій довжині блоку. При довжині блоку в 63 розряди вперше коди ІКВ володіють кращими коригувальними характеристиками. При збільшенні довжини блоку (пропорційно до порядку вибраного ІКВ) різниця коригувальних характеристик тільки зростає.

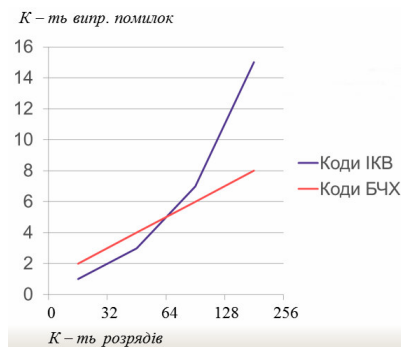


Рис. 1. Порівняння кодів ІКВ та БЧХ

Таким чином, встановлено співвідношення підбору оптимальних параметрів ІКВ для побудови завадостійкого кодування з кращими характеристиками та досліджено коригувальну здатність завадостійкого кодування на основі ІКВ (виправлення до 25% від довжини коду та виявлення до 50% від довжини коду). Порівняно характеристики завадостійкого кодування на основі ІКВ з кодуванням, базованим на кодах БЧХ, та встановлено покращення коригувальних характеристик на кодах ІКВ при довжині блоку 63 біт та більше.

[1]. Різник О.Я., Балич Б.І. Використання числових лінійок-в'язанок для кодування інформації. Інститутський вісник "Комп'ютерні науки та інформаційні технології", 2006. с.62-64.