УДК 519.15:621

О.Я. Різник, Д.Ю. Скрибайло-Леськів,
Х.Я. Заболотна, М.М. Красник

ЗАХИСТ ІНФОРМАЦІЇ НА ОСНОВІ ШУМОПОДІБНИХ КОДІВ

У даній роботі, з метою підвищення завадозахищеності сучасних інформаційних систем, розроблений регулярний і конструктивний метод синтезу шумоподібних кодів, що дозволило істотно підвищити параметричну скритність і захист інформації від несанкціонованого доступу.

Ключові слова: інформація, захист, завадозахищеність систем телекомунікацій, шумоподібний код

Вступ

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

У даній роботі, з метою підвищення завадозахищеності сучасних інформаційних систем, розроблений регулярний і конструктивний метод синтезу шумоподібних кодів, що дозволило істотно підвищити параметричну скритність і захист інформації від несанкціонованого доступу.

Науково-технічну основу появи сучасних телекомунікаційних мереж складає забезпечення максимальної пропускної спроможності систем передачі C при наявній смузі пропускання лінії зв'язку ΔF відповідно до формули Найквіста, одержаної з використанням теореми В.О. Котельнікова:

$$C = 2\Delta F \log M, \text{ [біт/с]}, \qquad (1)$$

де M – кількість дискретних значень сигналу.

Дана формула справедлива за умов відсутності шумів в лінії зв'язку.

Практично в лінії зв'язку мають місце завади (шуми), що приз-

 ISSN 1562-9945

водять до помилок при передачі інформації. Тоді максимальна пропускна спроможність системи передачі буде визначатись формулою Шеннона:

$$C = \Delta F \log(1 + \frac{P_с}{P_ш}), \text{ [біт/с]}, \quad (2)$$

де $P_с$, $P_ш$ - середня потужність коду та завад (шумів).

Важливою вимогою для цифрових систем передачі є забезпечення максимальної завадостійкості систем, яка залежить також від виду використаної модуляції (найкращу завадостійкість забезпечує багатопозиційна частотна маніпуляція).

Для підвищення завадостійкості систем передачі використовують завадостійке кодування, при якому до інформаційного повідомлення додають зайві перевірочні біти для виправлення помилок, що однак призводить до розширення спектру сигналу. Найбільше поширення набули блокові коди БЧХ (Боуза-Чоудхурі-Хоквенгема), коди Ріда-Соломона, а також безперервні згорткові коди з декодуванням їх за алгоритмом Вітербі.

Постановка задачі

Особливо цікавим є об'єднання методів кодування і шифрування. Можна стверджувати, що по суті кодування - це елементарне шифрування, а шифрування - це елементарне завадостійке кодування.

Розробка і реалізація таких універсальних методів - перспектива сучасних інформаційних систем.

Особливість шумоподібних кодів полягає в тому, що він створює шумоподібний спектр кодової послідовності (найбільш наближена до псевдовипадкової послідовності), а їх взаємна кореляція мінімальна. Найкращим кодом для створення шумоподібної послідовності є код Баркера, але він має велику надлишковість. Для її зменшення побудуємо шумоподібні коди на основі лінійок Голомба.

Корисною особливістю систем з шумоподібним сигналом є їх високі конфіденційність і завадостійкість, особливо до вузькосмугових завад. У основі техніки шумоподібних кодів лежить використання в каналі зв'язку для перенесення інформації декількох реалізацій цих кодів, розділення яких на прийомі здійснюється за допомогою селекції їх послідовності.

При цьому упевнене виявлення таких кодів може бути отримане при введенні надмірності, тобто при використанні для передачі повідомлень послідовності істотно надлишкової, ніж займає передане повідомлення.

Перевагою шумоподібного коду є можливість застосовувати новий вигляд селекції – за допомогою послідовності. Цікавою особливістю систем з шумоподібними кодами є її адаптивні властивості - із зменшенням числа завад завадостійкість зростає.

Опис методу кодування

Слабке місце багатьох систем кодування - це статистична слабкість коду, тобто, аналізуючи статистику за деякий період, можна скласти думку про те, що це за система і тоді діяти більш направлено. Тобто різко скорочується час пошуку ключа. Дана система оперує шумоподібними кодами, які по своїх властивостях, у тому числі і статистичним, практично ідентична білому шуму Гауса.

Властивості цих послідовностей:

у кожному періоді послідовності число 1 і 0 відрізняється не більш, ніж на одиницю;

серед груп з послідовних 1 і 0 в кожному періоді половина має тривалість в один символ, четверта частина має тривалість в два символи, восьма частина має тривалість в чотири символи і так далі.

кореляційна функція послідовності має єдиний значний пік амплітуди 1 і при всіх зрушеннях рівна $1/m$ (m - довжина послідовності).

кореляція між векторами обчислюється за формулою:

$$\rho(\chi, y) = \frac{A - B}{A + B} \qquad (3)$$

де A - число позицій, в яких символи послідовностей x і y збігаються;

B - число позицій, в яких символи послідовностей x і y різні.

У математиці оптимальною лінійкою або лінійкою Голомба називається набір невід'ємних цілих чисел, розташованих у вигляді ділень на уявній лінійці таким чином, що відстань між будь-якими двома діленнями є унікальною. Іншими словами, на всьому протязі лінійки, не можна знайти два числа, різниця між якими повторювалася б двічі [1, 2].

Число ділень на лінійці Голомба називають її порядком, а найбільшу відстань між двома її діленнями - довжиною. Інколи лінійки Голомба описуються відстанями між сусідніми діленнями, а не абсолютними координатами ділень. Максимальне число пар, які можна скласти з ділень лінійки порядку n, рівне:

$$\binom{n}{2} = \frac{n(n-1)}{2}. \qquad (4)$$

Тому в канонічному представленні лінійки Голомба найменше ділення відповідає нульовій координаті, а наступне за ним ділення розташовується на найменшій з двох можливих відстаней. Зовсім не обов'язково, що лінійка Голомба здатна виміряти всі відстані в межах її довжини, проте якщо це так, то таку лінійку називають досконалою. Проте, досконалі лінійки існують лише для порядків менших п'яти.

Лінійку Голомба називають оптимальною, якщо не існує коротших лінійок того ж порядку. Іншими словами, лінійка називається оптимальною, якщо значення її останнього ділення мінімально можливе [1].

При проведенні досліджень на послідовності елементів кожній j -й упорядкованій парі чисел (p_j,q_j); $p_j,q_j \in \{1,2,\ldots,N\}$ ставиться у відповідність сума $L_j = L(p_j,q_j)$ на послідовності цілих додатних чисел $K_N = (k_1,k_2,\ldots,k_i,\ldots,k_N)$ (табл. 1):

$$L_j = L(p_j,q_j) = \sum_{i=p_j}^{q_j} k_j\ ,\ \ p_j \le q_j \qquad (5)$$

Максимально можлива кількість L_N сум на послідовності чисел, значення яких відрізняються між собою, визначається тривіальною залежністю:

$$L_N = \frac{N(N+1)}{2}. \qquad (6)$$

В загальному випадку простою лінійкою Голомба порядку N на послідовності N чисел, називається така послідовність $K_N = (k_1, k_2, \ldots, k_i, \ldots, k_N)$, на якій суми набирають значень всіх L_N чи-

сел, починаючи зі заданого числа. В більш простому варіанті ці суми вичерпують значення чисел натурального ряду $1, 2, \ldots, L_N$.

Таблиця 1

Значення можливих сум для N елементів лінійки Голомба

	q_j							
p_j	1	2	…	$l-1$	l	…	$N-1$	N
1	k_1	k_2	…	k_{l-1}	k_l	…	k_{N-1}	k_N
2		$\sum_{i=1}^{2} k_i$	…	$\sum_{i=1}^{l-1} k_i$	$\sum_{i=1}^{l} k_i$	…	$\sum_{i=1}^{N-1} k_i$	$\sum_{i=1}^{N} k_i$
…				…	…	…	…	…
$l-1$				$\sum_{i=l-1}^{l} k_i$	$\sum_{i=l-1}^{l} k_i$	…	$\sum_{i=l-1}^{N-1} k_i$	$\sum_{i=l-1}^{N-1} k_i$
l					$\sum_{i=l-1}^{l} k_i$	…	$\sum_{i=l}^{N-1} k_i$	$\sum_{i=l}^{N} k_i$
…								…
N								$\sum_{i=N-1}^{N} k_i$

Одним з практичних використань лінійки Голомба, є використання її у фазованих антенних решітках радіоантен, наприклад в радіотелескопах. Антени з конфігурацією [0 1 4 6] можна зустріти в базових станціях стільникового зв'язку стандарту CDMA.

Ми ж використаємо лінійки Голомба для генерації шумоподібних кодів, так як лінійка Голомба за визначенням повинна мати всі різні відліки, а при великих величинах її довжина вона стає подібною на послідовність шумоподібних кодів за їх визначенням [3].

Запропонований метод побудови шумоподібних кодів, заснований на перетворенні лінійок Голомба.

Для побудови шумоподібних кодів за допомогою лінійок Голомба порядка N кратності R виділимо рядок із L_N пронумерованих у зростаючому порядку клітинок одновимірного масиву і заповнимо інформаційними "одиницями" клітинки, номери яких збігаються з числами, визначеними з лінійки Голомба. У клітинки, що залишилися незаповненими, занесемо "нулі". Утворена послідовність одиниць і

нулів є L_N-розрядним шумоподібним кодом, циклічним зсувом якого можна одержати й решту дозволених комбінацій.

Прикладом такого коду є таблиця кодових комбінацій, складена за допомогою лінійки Голомба порядка $N=7$ кратності $R=1$ (табл. 2):

0 1 4 10 18 23 25.

Будь-яка з L_N різних кодових комбінацій шумоподібного коду містить точно N одиничних символів в однойменних розрядах, що випливає з властивостей лінійки Голомба. Решта $L_N - N$ кодових комбінацій шумоподібного коду містять нулі [2].

Мінімальна кодова відстань для шумоподібного коду визначається як:

$$d_{\min} = 2(N\text{-}2) \tag{7}$$

Число помилок, які можна виявити t_1, і число помилок, що можна виправити t_2 за допомогою шумоподібного коду, визначається мінімальною кодовою відстанню:

$$t_1 \le d_{\min} - 1 \tag{8}$$

$$t_2 \le (t_1 - 1)/2 \tag{9}$$

Формули для визначення кількості помилок, які можуть бути виправлені t_2 або виявлені t_1 за допомогою описаного шумоподібного коду:

$$t_1 \le 2N - 5, \tag{10}$$

$$t_2 \le N - 2 \tag{11}$$

У розглянутих випадках значення параметрів L_N і N не зв'язані між собою будь-якою аналітичною залежністю і можуть вибиратися довільно. При цьому виникає питання про встановлення оптимального співвідношення між L_N і N, за дотримання якого розглянутий шумоподібний код набуває додаткових переваг. Завадостійкість шумоподібного коду зростає зі збільшенням N при умові мінімізації довжини лінійки Голомба L_N.

Таблиця 2

Шумоподібні коди на основі лінійки Голомба з $N = 7$ та $R = 1$

1	1	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	1	0	1
1	1	1	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	1	0
0	1	1	1	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	1
1	0	1	1	1	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0
0	1	0	1	1	1	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0
0	0	1	0	1	1	1	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0
0	0	0	1	0	1	1	1	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0
0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	1
1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0
0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0
0	0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	0	0	1	0	0	0	0	0
0	0	0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	0	0	1	0	0	0	0
0	0	0	0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	0	0	1	0	0	0
0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	0	0	1	0	0
0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	0	0	1	0
0	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	0	0	1
1	0	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	0	0
0	1	0	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0	0
0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	0
0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0
0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	0	0	1	0
0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	0	0	1
1	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	0	0
0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1	0
0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1	1
1	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	1	0	1	1

Побудовані за допомогою лінійок Голомба шумоподібні коди дають змогу виявляти до $2N - 5$ або виправляти до $N - 2$ помилок.

Структурна схема системи прийому-передачі інформації з використанням шумоподібних кодів приведена на рис. 1.

 ISSN 1562-9945

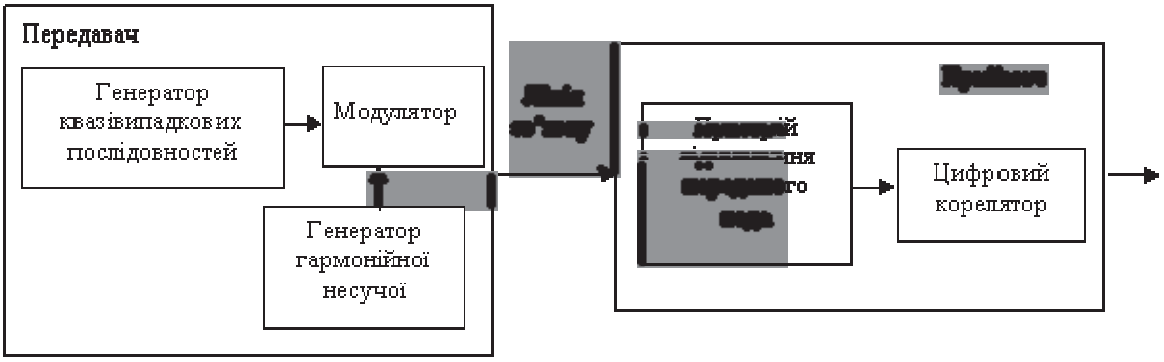

Рисунок 1 – Структурна схема системи прийому-передачі інформації

Основними апаратурними частинами прийомо-передаючої системи, які дозволяють відтворити переваги шумоподібних кодів є генератор квазівипадкових послідовностей (КВП) (у нашому випадку лінійок Голомба) і цифровий корелятор. Генератор квазівипадкових послідовностей визначає структуру шумоподібного коду, а цифровий корелятор здійснює узгоджений за структурою сигнала прийом. Генератори КВП прості в апаратурному виконанні. Можна сказати, що генератори шумоподібного коду не викликають утруднень при апаратурній реалізації, а самі шумоподібні коди мають гарні потенційні можливості для удосконалення трактів приймання-передачі.

Розроблений програмний продукт для кодування та декодування з виправленням помилок за допомогою шумоподібних послідовностей, де задаються:

– вхідні дані (елементи шумоподібної послідовності);

– кількість помилок, які знаходяться та виправляються;

– шлях до файлу, який необхідно закодувати та декодувати на основі шумоподібної послідовності.

Висновки

Шумоподобні коди відносяться до безлічі з украй нерегулярною розгалуженою структурою. Великий інтерес до цих кодів пов'язаний з тим, що їх аналоги, такі як квазікоди Баркера, лінійки Голомба, числові в'язанки знаходять використання в реальних завданнях, причому в типових, а не в екзотичних ситуаціях.

Дослідження різних типів шумоподібних кодових послідовностей свідчить про переваги тих із них, які синтезовані на основі лінійок Голомба, що дає змогу досягнути більшої криптостійкості та завадостійкості при перетворенні інформації в порівнянні з класичними шумоподібними кодовими послідовностями.

Розроблений алгоритм та програма спрощеного синтезу завадостійкої шумоподібної кодової послідовності на основі лінійок Голомба та створення ефективного алгоритму кодування і декодування інформації. Дослідження показують, що використання шумоподібних кодових послідовностей на основі лінійок Голомба в задачах перетворення інформації забезпечує простоту апаратурного застосування.

ЛІТЕРАТУРА

1. Різник В.В. Синтез оптимальних комбінаторних систем. - Львів, 1989.
2. Різник В.В., Різник О.Я., Кісь Я.П., Дурняк Б.В., Парубчак В.О.. Використання монолітних кодів в інформаційних технологіях. МНТК ISDMIT'2006, Євпаторія, т.2, с.39-42.
3. 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.

 ISSN 1562-9945