УДК 681.325.3

І.М. ЛАЗАРОВИЧ
Прикарпатський національний університет імені Василя Стефаника, м. Івано-Франківськ

РЕАЛІЗАЦІЯ МЕТОДІВ СИГНАЛЬНОЇ РАНДОМІЗАЦІЇ ДЛЯ ЗАВАДОСТІЙКОГО ПЕРЕДАВАННЯ ДАНИХ

В роботі наведено застосування процедури рандомізації для цифрової обробки сигналів, запропоновано використання рандомізації для перетворення фазоманіпульованого сигналу в близький до псевдовипадкового. Наведено структуру цифрового рандомізатора та алгоритм формування ключів рандомізації. Проведено дослідження запропонованих рішень на основі розробленої програмної моделі.

Ключові слова: кореляція, програмна модель, рандомізація, сигнал, сигнальний процесор, цифрова обробка сигналів, шифрування, шумоподібний сигнал, хешування.

I.M. LAZAROWYCH
Vasyl Stefanyk Precapathian National Univercity, Ivano-Frankivsk, Ukraine

IMPLEMENTATION OF THE SIGNAL RANDOMIZATION METHOD FOR NOISE-IMMUNE DATA TRANSMISSION

Abstract – the aim of the article is research and application of randomization procedure for noise-immune data transmitting, development of digital randomizer structure and algorithm for generation of the randomization key.

In this paper grounded the urgency to develop the effective methods of data transfer in the conditions of intensive noises. Examined the randomization procedure to convert the waveform. Proposed to use this procedure to convert the harmonic signal into close to the pseudo-random. Transmitted data can be detected based on the evaluation of the correlation function of the resulting signal. Proposed the structure of digital randomizer, which is the basis for creating specialized signal processor-based programmable logic circuits. Proposed the algorithm of the generating of randomization key for signal transformation with the shape of pseudo-random sequence.

The effectiveness of the method tested on basis of the created program model. According to the simulation method provides reliable data transmission with phase-shift keying (PSK) signals when the signal/noise ratio up to 0.35-0.4.

Keywords: correlation, program model, randomization, signal, signal processor, digital treatment of signals, encrypting, noise-like signal, randomization.

Вступ

Сьогоднішня інформатизація суспільства супроводжується надзвичайно швидкими темпами зростання об’ємів даних. Світові дослідження показують, що кожного року кількість продукованої людством інформації зростає приблизно на 50–70%, і згідно з прогнозами до 2020 року сягатиме 50 трлн гігабайт (50 зетабайт). Ці неймовірні інформаційні потоки передаються через різнотипні канали зв’язку, тому дедалі більш гостро стає проблема якісного і надійного приймання даних. Зокрема, для якісного передавання даних сьогодні часто використовують шумоподібні сигнали на основі М-послідовностей, послідовностей Баркера, Гоулда, Касамі [1]. Проте їх застосування пов’язано із рядом проблем, однією із яких є необхідність широкосмугових каналів зв’язку, що в цілому приводить до збільшення складності і вартості системи передавання. Водночас традиційні способи передавання даних на основі гармонічних вузькосмугових сигналів [2] не забезпечують належного рівня стійкості до завад та захищеності даних.

Тому задача пошуку, дослідження та застосування нових ефективних методів передавання даних, які відповідають сучасним потребам і вимогам, є актуальною.

Постановка завдання

В роботі [3] запропоновано використати рандомізацію для завадостійкого передавання сигналів. Метою даної роботи є реалізація методу сигнальної рандомізації для завадостійкого передавання даних у системах із вузькосмуговими каналами зв’язку. Для реалізації мети потрібно виконати наступні етапи:

- формалізувати суть методу;
- розробити структуру цифрового рандомізатора;
- розробити алгоритм формування ключів для сигнальної рандомізації;
- перевірити ефективність запропонованих рішень.

Результати дослідження

Рандомізація (англ. *random* – випадковий, нерегулярний, безпорядковий) – це нелінійна процедура навмисного внесення “випадковості” або шумоподібності в обробку вибіркових даних для перетворення деяких систематичних помилок у випадкові. Рандомізація полягає в перемішуванні інформаційної вибірки відповідно до певного закону. В контексті шифрування інформації цю процедуру називають перемішуванням, при організації доступу до пам’яті – хешуванням (обробка на основі *hash*-функцій)[3].

Оператор рандомізації $\Re\text{an}$ послідовності $X = \{x_1, x_2, \ldots, x_i, \ldots x_n\}$ позначає дію, яка полягає в переміщенні i -го елемента на місце j -го елемента послідовності X, а відповідність між i та j називають

законом рандомізації [4]:

$$X = \{x_i\}, \quad \Re\text{an}(X) = \Re\text{an}(\{x_i\}) = X^{\Re\text{an}}, \tag{1}$$

$$X^{\Re\text{a}} = \{x_j\}, \ i = \overline{1,n}, \ j = k_i. \tag{2}$$

де $K = \{k_i\}$ – масив-ключ рандомізації $\Re\text{an}$.

В результаті рандомізації послідовності X утворюється послідовність $Y = \{y_1, y_2, \ldots, y_j, \ldots y_n\}$, причому $x_i = y_j$, $i = \overline{1,n}$, $j = \overline{1,m}$.

Існує очевидна процедура $\Re\text{an}^{-1}$ обернена до $\Re\text{an}$, тобто така, що дозволяє отримати початкову послідовність з рандомізованої, тобто:

$$\Re\text{an}^{-1}(Y) = X. \tag{4}$$

Якщо пряма процедура $\Re\text{an}$ виконується згідно виразу $y_i = x_{s_i}$, тоді процедура $\Re\text{an}^{-1}$ виконується так:

$$\Re\text{an}^{-1} : z_{s_i} = y_i. \tag{5}$$

де $S = \{s_i\}$ – масив-ключ (закон) рандомізації. Очевидно, що $z_i = x_i$, тому процедура рандомізації є зворотною.

Рандомізація дозволяє виконати перетворення форми сигналу, зокрема за її допомогою можна сформувати сигнал, який по своїй формі і властивостях кореляційної функції наближений до псевдовипадкового. У роботі [3] пропонується використовувати рандомізацію для завадостійкого передавання інформації з використанням фазової маніпуляції гармонійних сигналів.

Структурна схема, яка відображає функціонування методу наведена на рис. 1.

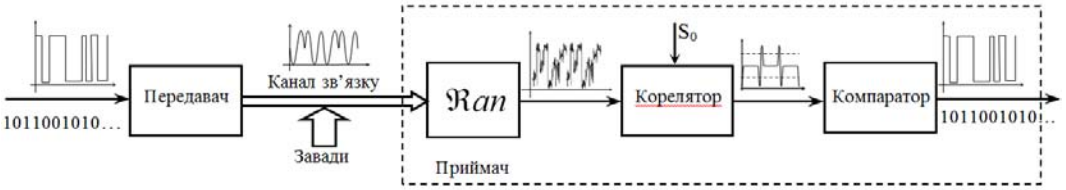

Рис. 1. Структура системи передавання з рандомізацією

Нехай від джерела інформації надходить бітова послідовність. Передавач формує фазоманіпульований вихідний сигнал, зсув фази складає 180°. Канал зв'язку піддається впливу адитивного шуму. Перший етап обробки зашумленого сигналу в приймачі – виконання рандомізації відповідно до заданого ключа. Ключ рандомізації формується таким чином, щоб результуючий сигнал по формі був наближений до псевдовипадкового. Далі корелятор порівнює прийнятий рандомізований і взірцевий сигнал нуля чи одиниці. Якщо значення кореляції виходить за межі встановленої апертури, то це свідчить про приймання сигналу відповідного логічного рівня [3, 4]. Згідно з проведеними дослідженнями на основі програмної моделі, що реалізує запропонований метод, міра стійкості до завад визначається вибраним ключем рандомізації та правильністю вибору апертури.

Структура цифрового рандомізатора

З метою реалізації запропонованого методу було розроблено структуру рандомізатора (рис.2), який виконує перетворення форми вхідного сигналу приймача $X=\{x_i\}$ по наперед заданому закону $K=\{k_i\}$, $i = \overline{1,m}$, де m– довжина ключа.

Перед початком роботи рандомізатора необхідно виконати початкову ініціалізацію схеми, шляхом подання високого логічного рівня на коло *Reset*. При цьому відбувається обнулення лічильників *CT*1 та *CT*2, а також регістра *RG*. На вхід *Clock* подається сигнал тактування роботи АЦП, яке перетворює відліки аналогового сигналу x_i в відповідний n-розрядний двійковий код, що формується на його виходах $Q_1 ... Q_n$.

Двійковий лічильник *CT*1 призначений для адресування постійної пам'яті *PROM*, в якій міститься ключ-закон рандомізації *K*. Двійковий лічильник *CT*2 призначений для адресування динамічної пам'яті *RAM*, в якій містяться рандомізовані дані. Значення лічильників *CT*1 та *CT*2 інкрементуються при поступленні на їх входи *C* фронту спадання із виходу *DE* АЦП.

Логічні елементи в схемі призначені для інвертування та часової затримки сигналу АЦП *DE*. Регістр *RG* містить *i*-й відлік рандомізованих даних.

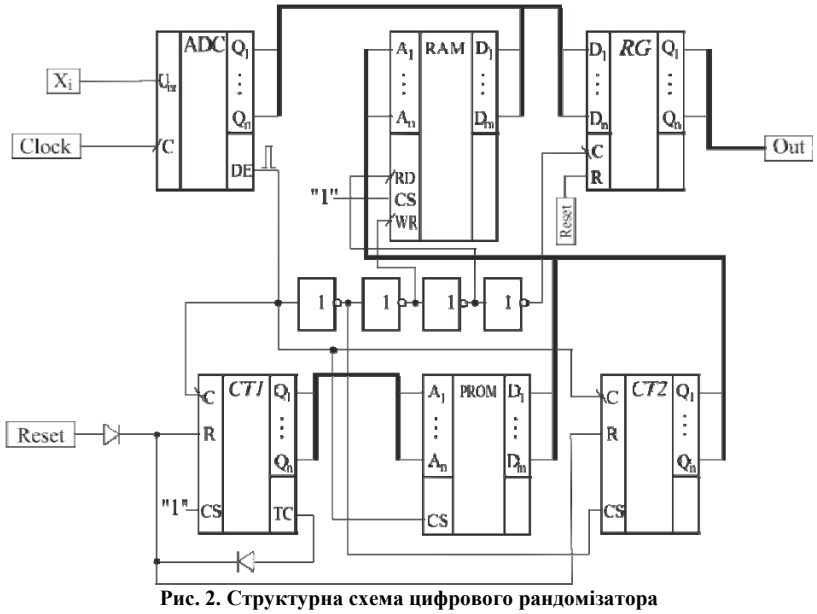

Рис. 2. Структурна схема цифрового рандомізатора

Після готовності даних АЦП формує сигнал *DE* (*Data Enabled*) який поступає на його вхід *CS* (*Chip Select*), що дозволяє сигнали на виході АЦП, а також на вхід *CS* пам'яті *PPOM*. В пам'ять *RAM* по адресу з пам'яті ключів *PROM*, що адресується поточним значенням лічильника *CT*1, записується *n*-розрядне число з виходу АЦП. По фронту спаду сигналу *DE* інкрементуються лічильники *CT*1 та *CT*2, забороняється вихід *PROM* і дозволяється вихід *CT*2. Далі відбувається запис *n*-розрядного рандомізованого числа із пам'яті *RAM*, що адресується лічильником *CT*2 в регістр *RG*. Тривалість існування поточного рандомізованого відліку на виходах $Q_1...Q_n$ регістра *RG* рівна часу оцифрування АЦП. Далі після готовності наступної порції даних на виході АЦП робота схеми продовжується аналогічним чином.

Алгоритм формування ключів для рандомізації

Згідно з проведеними дослідженнями на основі програмної моделі цифрової системи передавання даних з рандомізацією, найкращих показників завадостійкості можна досягнути при використанні перетворення форми початкового сигналу до псевдовипадкового, наприклад можна використати М-послідовність [5]. Якщо N – кількість біт М-послідовності, то об'єм вибірки дискретизованих значень одного періоду фазоманіпульованого сигналу $X=\{x_i\}$ визначається як $m=rN$, де r – парне число, яке позначає коефіцієнт розширення М-послідовності. Тоді алгоритм формування ключа $K=\{k_i\}$, $i=\overline{1,m}$, демонстрація якого для М-послідовності 1110100 наведена на рис.3, складається з наступних кроків:

1. Формування діапазонів індексів, які відповідають значенням "1" у М-послідовності: [0, 3r-1] та [4r, 5r-1];
2. Визначення центрів «одиничних» діапазонів: $d_1=3r/2$ та $d_2=4r+r/2$;
3. Визначення індексів $j_{1,0}$ та $j_{2,0}$ для двох елементів, що мають максимальне значення серед x_i;
4. Запис значень індексів $j_{1,0}$ та $j_{2,0}$ в масив K на позиції d_1 та d_2;
5. Визначення індексів $j_{1,Z1}$ та $j_{2,Z2}$ для двох елементів, що мають максимальне значення серед x_i, за винятком попередньо знайдених елементів;
6. Запис значень індексів $j_{1,Z1}$ та $j_{2,Z2}$ в масив K на позиції d_1+gz_1 та d_2+gz_2, де z_1 та z_2 – номер ітерації для відповідного «одиничного» діапазону, а g – це змінна, що приймає значення +1 або -1, та змінюється на протилежну на кожній ітерації;
7. Циклічне повторення кроків 5-6, поки z_1 знаходиться в межах [0, 3r-1], а z_2 – в межах [4r, 5r-1];
8. Повторення кроків 1–7 для діапазонів індексів, які відповідають значенням "0" в М-послідовності.

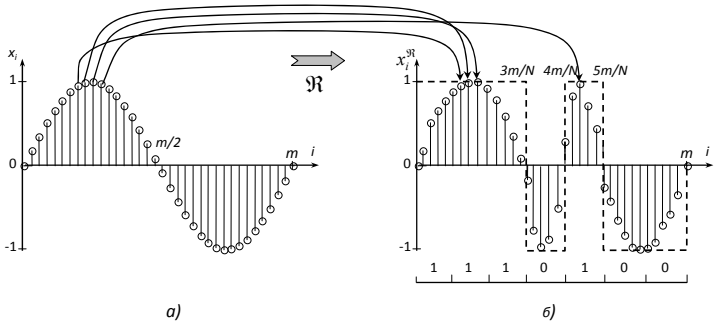

Рис. 3. Реалізація алгоритму рандомізації

Запропонований алгоритм був реалізований в середовищі C++ Builder 2010 у вигляді програмної моделі системи передавання даних з рандомізацією. В якості адитивної завади, яка діє на канал зв'язку було використано білий гаусів шум AWGN [6]. В якості міри ефективності методу було обрано відношення $P_c/P_ш$. Моделювання показало, що метод працює при значеннях $P_c/P_ш$ аж до 0,35-0,4, забезпечуючи при цьому безпомилкове передавання інформації, довжина М-послідовності, що використовувалась – 15 і 31 біт.

Висновки

Таким чином, запропонований спосіб передавання даних є ефективним з точки зору стійкості до завад і дозволяє приймати сигнали при інтенсивності шумів, що в 3 рази перевищує рівень корисного сигналу. При цьому в канал зв'язку подається фазоманіпульований сигнал, який не вимагає широкої смуги пропускання. Наведена в роботі схема цифрового рандомізатора є простою для апаратної реалізації (наприклад на основі ПЛІС) і дозволяє отримувати рандомізовані дані в реальному режимі часу. Запропоновані рішення можуть бути використані для передавання даних в системах управління і автоматики, в комп'ютерних мережах та інших телекомунікаціних системах, що працюють в умовах інтенсивних завад.

Література

1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение / Скляр Бернард ; [пер. с англ.]. – Изд. 2-е, испр. – М. : Издательский дом «Вильямс», 2003. – 1104 с.

2. Феер К. Беспроводная цифровая связь: методы модуляции Феер К. / под. ред. В. И. Журавлёва ; [пер. с англ.]. – М. : Радио и связь, 2000. — 520 с.

3. Метод передавання цифрових даних з використанням рандомізації на основі багаторівневих М-послідовностей // Наукові вісті Інституту менеджменту та економіки "Галицька академія" (технічні науки). Івано-Франківськ : Інститут менеджменту та економіки "Галицька академія", 2007. – № 2(12). – С. 77–79.

4. Моделювання цифрового приймача сигналів з використанням рандомізації на основі багаторівневих М-послідовностей // Вісник Хмельницького національного університету (технічні науки).– Хмельницький : ХНУ, 2010. – № 5. – С. 180–184.

5. Варакин Л.Е. Системы святи с шумоподобными сигналами / Варакин Л.Е. – М. : Радио и связь, 1985. – 384 с.

6. Голдсмит А. Беспроводные коммуникации / А. Голдсмит. – М. : Техносфера, 2011. – 904 с.

References

1. Sklyar, Bernard. Tsifrovaya svyaz. Teoreticheskie osnovyi i prakticheskoe primenenie. Izd. 2-e, ispr. : Per. s angl. – M. : Izdatelskiy dom «Vilyams», 2003. – 1104 s.

2. Feer K. Besprovodnaya tsifrovaya svyaz: metodyi modulyatsii. — Per. s angl. // Pod. red. V. I. ZhuravlYova. — M.: Radio i svyaz, 2000. — 520 s.

3. Metod peredavannia tsyfrovykh danykh z vykorystanniam randomizatsii na osnovi bahatorivnevykh M-poslidovnostei // Naukovi visti Instytutu menedzhmentu ta ekonomiky "Halytska akademiia" (tekhnichni nauky). – 2007. – 2(12). – Ivano-Frankivsk: Instytut menedzhmentu ta ekonomiky "Halytska akademiia", 2007. – S. 77-79.

4. Modeliuvannia tsyfrovoho pryimacha syhnaliv z vykorystanniam randomizatsii na osnovi bahatorivnevykh M-poslidovnostei // Visnyk Khmelnytskoho natsionalnoho universytetu (tekhnichni nauky). – 2010. – 5. – Khmelnytskyi: KhNU, 2010. – S. 180 – 184.

5. Varakin L.E. Sistemyi svyati s shumopodobnyimi signalami. – M.: Radio i svyaz, 1985. – 384 s.

6. Goldsmit A. Besprovodnyie kommunikatsii / A. Goldsmit. - M.: Tehnosfera, 2011. - 904 s.

Рецензія/Peer review : 27.10.2014 р. Надрукована/Printed :29.11.2014 р.
Рецензент: д.ф-м.н. проф. П.В. Філевич