УДК 621.396.001 (519.2)

ПІДВИЩЕННЯ РІВНЯ ЗАХИЩЕНОСТІ ДАНИХ В СИСТЕМІ ЗВ'ЯЗКУ З ФАЗОВОЮ МАНІПУЛЯЦІЄЮ ШУМОВОГО СИГНАЛУ

Дідковський Р.М., к.т.н., Метелап В.В.

Черкаський державний технологічний університет

В статті запропонована методика побудови ортогонального перетворення шумового сигналу, що не змінює середнього значення та дисперсії сигналу. Застосування даного перетворення в системах зв'язку з фазовою маніпуляцією шумового сигналу дозволяє приховати кореляційні зв'язки між опорним та інформаційним сигналами, що підвищує рівень захищеності інформації.

В статье предложена методика построения ортогонального преобразования шумового сигнала, которая не изменяет среднего значения и дисперсии сигнала. Применение данного преобразования в системах связи с фазовой манипуляцией шумового сигнала позволяет скрыть корреляционные связи между опорным и информационным сигналами, что повышает уровень защищенности информации.

В статье предложена методика построения ортогонального преобразования шумового сигнала, которая не изменяет среднего значения и дисперсии сигнала. Применение данного преобразования в системах связи с фазовой манипуляцией шумового сигнала позволяет скрыть корреляционные связи между опорным и информационным сигналами, что повышает уровень защищенности информации.

Постановка задачі. Розвиток технології цифрової обробки сигналів в останні два десятиліття дозволив по новому підійти до використання шумових сигналів в якості носія інформації. Підтвердженням актуальності досліджень у даному напрямку є значний інтерес дослідників різних країн до побудови систем зв'язку з шумовими та хаотичними сигналами [1-5].

Системи зв'язку з шумовими сигналами наслідують всі позитивні якості традиційних надширокополосних систем і, крім того, мають підвищений рівень захищеності даних від несанкціонованого доступу.

Однією з найбільш завадостійких є система з фазовою маніпуляцією шумового сигналу [6-7]. Структурна схема такої системи зображена на рис. 1.

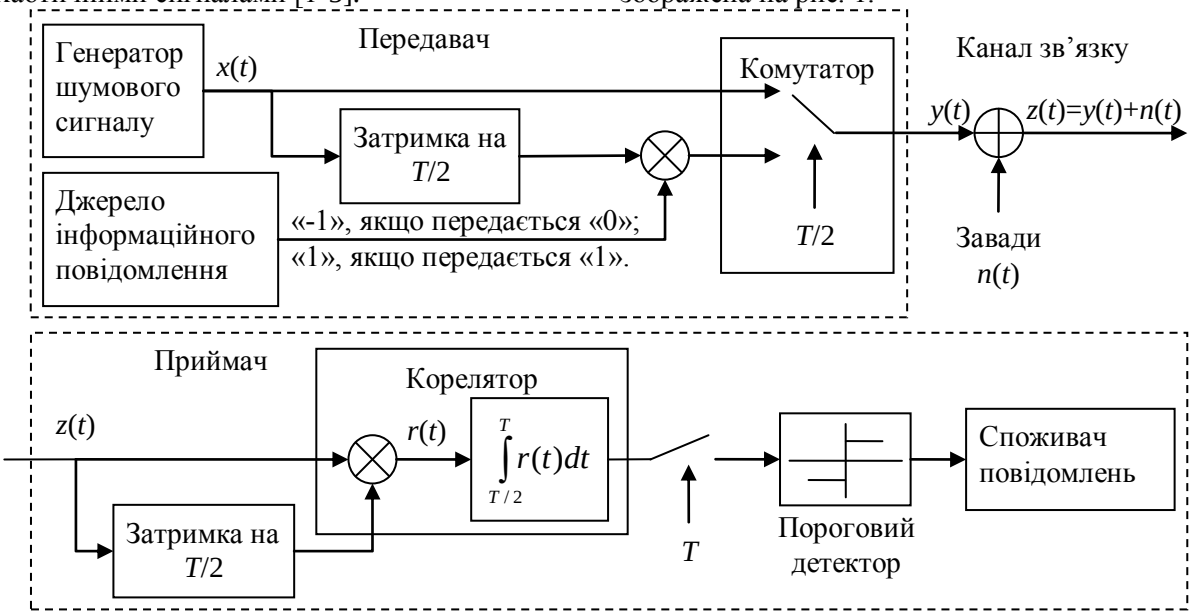

Рис. 1 – Структурна схема системи зв'язку з фазовою маніпуляцією шумового сигналу.

Якщо вважати, що формування і обробка шумового сигналу в даній системі здійснюється цифровими методами в дискретному часі, то сигнал $x(t)$ на виході генератора шуму, що спостерігається протягом передачі одного біта інформації буде представлений у вигляді вектора $(x_1, x_2, ..., x_{2n})$.

Координати цього вектора є реалізаціями однаково розподілених випадкових величин з нульовим математичним сподіванням, а розмірність вектора визначається рівністю $2n = T/\Delta t$, де T – тривалість бітового інтервалу, Δt – період тактового генератора системи.

Тоді сигнал $y(t)$ на виході передавача запишеться у вигляді

$$y_k = \begin{cases} x_k, & k = 1,2,...,n, \\ \alpha\, x_{k-n/2}, & k = n+1, n+2, ..., 2n, \end{cases}$$

де множник $\alpha = -1$ при передачі «0» та $\alpha = 1$ при передачі «1».

Першу половину сигналу $y(t)$ називаємо опорним сигналом, а другу – інформаційним.

Якщо символи «0» і «1» в інформаційному повідомленні зустрічаються рівноімовірно, то за рахунок взаємної компенсації позитивної та негативної кореляції опорного і інформаційного сигналу ні спектральний ні кореляційний аналіз сигналу $y(t)$ не дає можливості визначити швидкість передачі даних.

Не маючи точних даних щодо швидкості передачі даних (яка визначається тривалістю бітового інтервалу) не можливо синхронізувати приймач, а значить не можливо отримати доступ до даних.

Однак, після піднесення сигналу $y(t)$ до квадрату всі кореляційні зв'язки між опорними та інформаційними фрагментами сигналу стають позитивними. Тому обчислення автокореляційної функції (АКФ) сигналу $y^2(t)$ дозволяє чітко визначити довжину бітового інтервалу.

На рис. 2 зображено типову реалізацію АКФ сигналу $y^2(t)$. В точці, що відповідає приросту часу $0.5T$, чітко проглядається пік автокореляційної функції, який значно перевищує загальний шумовий рівень.

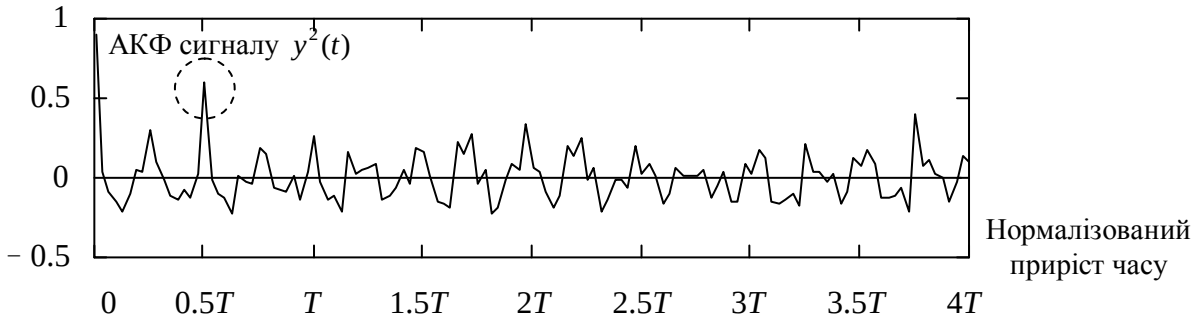

Рис. 2 – Автокореляційна функція квадрата модульованого сигналу.

Мета роботи. Поставимо задачу відшукання перетворення, застосування якого до інформаційної частини сигналу дозволило би надійно маскувати вказані кореляційні зв'язки.

Це перетворення має задовольняти кілька вимог:

1) має існувати обернене перетворення;
2) застосування перетворення має залишати незмінним математичне сподівання та дисперсію вектора;
3) перетворення має залежати від кількох ключових параметрів, лише знаючи які можна було би правильно відтворити сигнал на приймальній стороні.

Основна частина. Визначимо тип перетворення, яке б задовольняло поставленим вимогам.

Незмінність дисперсії сигналу еквівалентна незмінності модуля відповідного вектора. Поворот є одним із перетворень, що зберігають модуль вектора. Крім того, кути

повороту цілком можуть відігравати роль секретних параметрів перетворення. Тому саме поворот обраний для подальших досліджень.

Формулу обчислення середнього значення координат вектора можна записати у вигляді:

$$\bar{x} = \frac{1}{n}(x_1 + x_2 + ... + x_n) =$$

$$= \frac{1}{n}\langle (1,1,...,1)\cdot(x_1, x_2, ..., x_n)\rangle =$$

$$= \frac{1}{\sqrt{n}}\,\mathrm{np}_{(1,1,...,1)}(x_1, x_2, ..., x_n).$$

де символ $\mathrm{np}_{\bar{b}}\,\bar{a}$ означає проекцію вектора $\bar{a}$ на вектор $\bar{b}$.

Отже, незмінність середнього значення координат вектора $\bar{x}$ еквівалентна незмінності проекції цього вектора на вектор $(1,1,...,1)$. З точки зору повороту це означає, що поворот має здійснюватись навколо вектора $(1,1,...,1)$ (залишати цей вектор нерухомим).

Знаходження матриці A такого повороту виконаємо в два етапи:

1) побудова нового ортонормованого базису, перший вектор якого співнапрямлений вектору $(1,1,...,1)$, тобто має вигляд $\left(\frac{1}{\sqrt{n}}, \frac{1}{\sqrt{n}}, ..., \frac{1}{\sqrt{n}}\right)$;
2) побудова матриці M повороту, що залишає нерухомим перший базисний вектор;
3) знаходження матриці повороту в початковому базисі.

Побудова необхідного базису може бути здійснена виходячи з довільної лінійно незалежної системи векторів, перший вектор якої $\bar{e}_1 = (1,1,...,1)$. Виберемо, наприклад, базис виду (тут і далі будемо використовувати стовпцевий запис координат векторів):

$$\bar{e}_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ ... \\ 1 \end{pmatrix}, \bar{e}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ ... \\ 0 \end{pmatrix}, \bar{e}_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ ... \\ 0 \end{pmatrix}, ..., \bar{e}_n = \begin{pmatrix} 0 \\ 0 \\ 0 \\ ... \\ 1 \end{pmatrix}.$$

Проведемо для цієї системи процедуру ортогоналізації Грама-Шмідта [8]:

$$\bar{e}'_1 = \bar{e}_1, \quad \bar{e}'_2 = \bar{e}_2 - \frac{<\bar{e}_2 \cdot \bar{e}_1>}{\bar{e}_1^2}\cdot\bar{e}_1,$$

$$\bar{e}'_3 = \bar{e}_3 - \frac{<\bar{e}_3 \cdot \bar{e}_1>}{\bar{e}_1^2}\cdot\bar{e}_1 - \frac{<\bar{e}_3 \cdot \bar{e}'_2>}{\bar{e}'^2_2}\cdot\bar{e}'_2, \ ...,$$

$$\bar{e}'_n = \bar{e}_n - \frac{<\bar{e}_3 \cdot \bar{e}_1>}{\bar{e}_1^2}\cdot\bar{e}_1 - \frac{<\bar{e}_3 \cdot \bar{e}'_2>}{\bar{e}'^2_2}\cdot\bar{e}'_2 - ...$$

$$... - \frac{<\bar{e}_3 \cdot \bar{e}'_{n-1}>}{\bar{e}'^2_{n-1}}\cdot\bar{e}'_{n-1}.$$

Отриманий базис $\bar{e}'_1$, $\bar{e}'_2$, $\bar{e}'_3$, …, $\bar{e}'_n$ – ортогональний, але не ортонормований. Після нормалізації за формулами

$$\bar{e}''_i = \frac{1}{|\bar{e}'_i|}\cdot\bar{e}'_i, \ i = 1,2,...,n$$

остаточно маємо ортонормований базис $\bar{e}''_1$, $\bar{e}''_2$, $\bar{e}''_3$, …, $\bar{e}''_n$.

Координати векторів цього базису об'єднаємо в матрицю переходу C.

Дана матриця має наступні властивості:

1) $|C| = 1$;
2) $C^{-1} = C^T$, тобто $C \cdot C^T = E$ – одинична матриця.

Зауважимо, що змінюючи початковий набір векторів (окрім першого вектора), наприклад, переставляючи вектори місцями, можемо отримати значний набір матриць C. Вибір однієї із цих матриць для використання в поточному сеансі зв'язку може бути одним із секретних параметрів.

Більш простий метод побудови матриці C базується на використанні матриці Адамара. Використаємо матрицю Адамара H впорядковану за Уолшем (по частості). Її елементи обчислюються за формулами [9]:

$$h_{m,u} = (-1)^{<m,r(u)>},$$

де $<m, r(u)> = \sum_{s=0}^{k-1} m_s \cdot r_s(u)$, $k = \log_2 n$,

$r_0(u) = u_{k-1}$, $r_1(u) = u_{k-1} + u_{k-2}$,

$r_2(u) = u_{k-2} + u_{k-3}$, …, $r_{k-1}(u) = u_1 + u_0$,

u_s і m_s – коефіцієнти двійкового зображення чисел u і m, тобто

$$u = u_{k-1}2^{k-1} + u_{k-2}2^{k-2} + ..u_1 2^1 + u_0 2^0,$$

$$m = m_{k-1}2^{k-1} + m_{k-2}2^{k-2} + ...m_1 2^1 + m_0 2^0.$$

Перевагою матриці H є те, що вона симетрична, тобто $H = H^T$. Крім того, модулі всіх векторів-стовпців цієї матриці однакові і

рівні $\sqrt{n}$, тому для отримання матриці переходу C достатньо провести нормалізацію за формулою

$$C = \frac{1}{\sqrt{n}} \cdot H .$$

Для такої матриці C виконується рівність $C^{-1} = C^T = C$, тобто ця матриця є оберненою до самої себе.

Сформуємо тепер матрицю повороту.

Будь-який поворот є суперпозицією елементарних поворотів [8]. Насамперед побудуємо матрицю виду

$$M' = \begin{pmatrix} 1 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & -1 & \dots & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & 0 & -1 \\ 0 & 0 & 0 & 0 & \dots & 1 & 0 \end{pmatrix}.$$

Ця матриця визначає суперпозицію поворотів на кут $\pi/2$ в площинах, які визначені парами базисних векторів $\bar{e}_3''$ і $\bar{e}_4''$, $\bar{e}_5''$ і $\bar{e}_6''$, …, $\bar{e}_{n-1}''$ і $\bar{e}_n''$. Дане перетворення забезпечує те, що образ вектора буде близьким до ортогонального відносно початкового вектора.

Побудуємо матрицю M'', що відповідає суперпозиції q поворотів на кути α_1, α_2, …, α_q в площинах базисних векторів $\bar{e}_{r_1}''$ і $\bar{e}_{s_1}''$, $\bar{e}_{r_2}''$ і $\bar{e}_{s_2}''$, …, $\bar{e}_{r_q}''$ і $\bar{e}_{s_q}''$. Для цього в одиничній матриці E відповідної розмірності замінимо елементи за наступними формулами

$$m_{r_i,r_i} = \cos\alpha_i,\ m_{r_i,s_i} = -\sin\alpha_i,$$

$$m_{s_i,r_i} = \sin\alpha_i,\ m_{s_i,s_i} = \cos\alpha_i,$$

де $i = 1,2,...,q$. Знання вибору значень кутів α_i та номерів r_i і s_i є ключем необхідним для правильного відновлення інформаційної частини сигналу та прийому і детектування сигналу загалом.

Остаточно матрицю повороту знайдемо за формулою

$$M = M'' \cdot M' .$$

Перетворення, що відповідає матриці M здійснює композицію всіх поворотів, описаних вище.

Ця матриця перетворення записана в базисі $\bar{e}_1''$, $\bar{e}_2''$, $\bar{e}_3''$, …, $\bar{e}_n''$.

Необхідно отримати матрицю перетворення в початковому базисі (що визначається одиничною матрицею), в якому записані координати вектора-сигналу. Для цього скористаємося формулою [8]:

$$A = C \cdot M \cdot C^T .$$

За побудовою дане перетворення зберігає середнє значення та дисперсію сигналу.

Позначимо $\bar{s}$ вектор, що відповідає дискретному представленню сигналу, який підлягає перетворенню (прообраз), а $\bar{s}'$ – образ цього вектора. В якості матриці перетворення використаємо матрицю A, отриману вище. Тоді

$$\bar{s}' = A \cdot \bar{s} . \qquad (1)$$

Відновлення сигналу відбувається за формулою

$$\bar{s}'' = A^T \cdot \bar{s}' = \bar{s} .$$

Найважливішим показником ефективності побудованого перетворення є значення коефіцієнту кореляції між образом і прообразом $r(\bar{s},\bar{s}')$. Дослідимо це питання за допомогою обчислювального експерименту.

В якості вектора $\bar{s}$ розмірності $n = 16$ візьмемо кортеж із 16-ти реалізацій нормально розподіленої випадкової величини з нульовим математичним сподіванням та одиничною дисперсією. За формулою (1) знайдемо вектор $\bar{s}'$ і обчислимо коефіцієнт кореляції $r(\bar{s},\bar{s}')$. Повторимо дослід 100000 раз і обчислимо середнє значення відповідного коефіцієнта кореляції. Отримаємо

$$\bar{r}(\bar{s},\bar{s}') = 0.067 .$$

При цьому дисперсія значення $r(\bar{s},\bar{s}')$ складає всього 0.023.

Отже, коефіцієнт кореляції образу і прообразу досить малий аби не дозволити виявити швидкість передачі даних в системі.

Обчислення автокореляційної функції при застосуванні побудованого перетворення дає аналогічний результат. На рис. 3 зображено фрагмент реалізації АКФ квадрата модульованого сигналу при застосуванні перетворення.

Як видно з рисунку, в даному випадку АКФ не містить характерних піків і має цілком шумовий характер.

Таким чином застосування запропонованого перетворення повністю досягає поставленої мети – маскування кореляційних зв'язків між опорним та інформаційним сигналом.

Зауважимо, що для реалізації даного підходу для підвищення захищеності даних в системах зв'язку з фазовою маніпуляцією шумового сигналу потрібна певна модифікація пристроїв передачі та приймання.

В передавачі між пристроєм затримки на $T/2$ та пристроєм множення має бути вбудований пристрій, що виконує пряме перетворення. А в приймачі між входом та пристроє множення має розміститися пристрій, що виконує обернене перетворення. При цьому алгоритми модуляції та демодуляції залишаються незмінними.

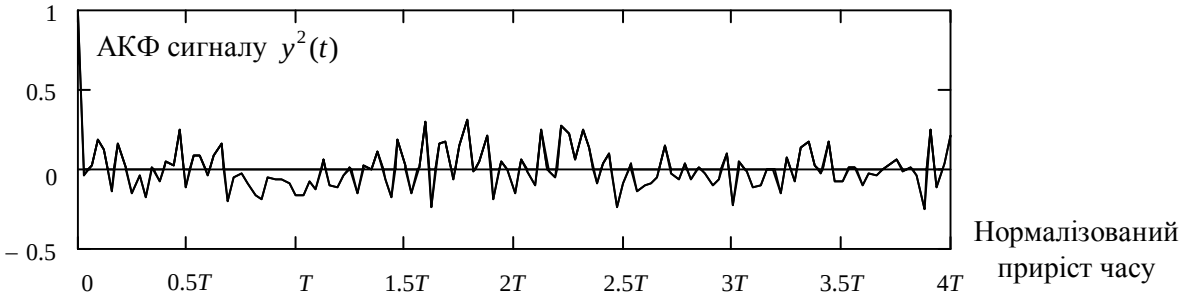

Рис. 3 – Автокореляційна функція квадрата модульованого сигналу при застосуванні перетворення.

Висновки. В роботі запропоновано принцип побудови ортогонального перетворення, яке залежить від ряду секретних параметрів та забезпечує зменшення рівня кореляції між опорним та інформаційним сигналом.

При цьому застосування перетворення не змінює середнього значення та дисперсії початкового сигналу.

Література:

1. L. Kocarev, K. S. Halle, K. Eckert, L. O. Chua, and U. Parlitz, "Experimental demonstration of secure communications via chaotic synchronization," Int. J. Bifurcation Chaos, vol. 2, no. 3, pp. 709–713, 1992.
2. K.M. Cuomo and A.V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications," Phys. Rev. Lett., vol. 71, pp. 65–68, 1993.
3. U. Parlitz, L.O. Chua, L. Kocarev, K.S. Halle, and A. Shang, "Transmission of digital signals by chaotic synchronization," Int. J. Bifurcation Chaos, vol. 2, pp. 973–977, 1992.
4. H. Dedieu, M. P. Kennedy, and M. Hasler, "Chaos shift keying: Modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuit," IEEE Trans. Circuits Syst. II, vol. 40, pp. 634–642, Oct. 1993.
5. G. Kolumbán, B. Vizvari,W. Schwarz, and A. Abel, "Differential chaos shift keying: A robust coding for chaos communications," in Proc., 4th Int. Workshop on Nonlinear Dynamics of Electronics Systems, (NDES'96), Seville, Spain, June 1996, pp. 87–92.
6. Первунінський С.М., Дідковський Р.М., Метелап В.В., Тобілевич Ю.Є. Математичне моделювання систем зв'язку з кореляційно-часовою модуляцією // Вісник Черкаського університету. Серія «Прикладна математика». ЧНУ. – 2006. – Випуск 83. – С.112-123.
7. Патент України №16305. Пристрій для передачі інформації шумовими сигналами / С.М. Первунінський, Р.М. Дідковський, В.В. Метелап. – МПК H04B 7/00, 2006, Бюл. №8.
8. Канатников А.Н., Крищенко А.П. Линейная алгебра: Учеб. для вузов. 3-е изд., стереотип. / Под ред. В.С. Зарубина, А.П. Крищенко. - М.: Изд-во МГТУ им. Н.Э. Баумана, 2002. - 336 с.
9. Бабак В.П., Хандецький В.С., Шрюфер Е. Обробка сигналів. – К.: Либідь, 1996. – 392 с.