DOI 10.31891/2307-5732-2020-287-4-192-198
УДК 621.391.01

М.О. СЛОБОДЯН, А.А. ТАРАНЧУК, В.Є. ГАВРОНСЬКИЙ
Хмельницький національний університет

ГЕНЕРУВАННЯ ШИРОКОСМУГОВИХ ХАОТИЧНИХ СИГНАЛІВ ДЛЯ ПРИХОВАНОЇ ПЕРЕДАЧІ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Стаття присвячена математичному моделюванню генератора широкосмугових хаотичних коливань на основі класичної нелінійної динамічної системи Лоренца. На базі двох синхронно зв'язаних динамічних генераторів Лоренца була побудована модель системи передачі інформації з хаотичним маскуванням довільного вузькосмугового сигналу широкосмуговим хаотичним сигналом. Чисельний розв'язок диференціальних рівнянь системи та амплітудний спектр вихідного сигналу хаотичного генератора було розраховано за допомогою програмного забезпечення Matlab. З метою дослідження зміни динамічного режиму залежно від параметрів моделі було розраховано спектр показників Ляпунова та побудовано діаграму біфуркацій. Модель системи синхронізації зв'язаних динамічних систем та модель генератора вузькосмугових сигналів з довільним типом модуляції були побудовані в середовищі імітаційного моделювання Simulink.

Ключові слова: *хаос, хаотичне маскування, динамічні системи, синхронізація.*

M. SLOBODIAN, A. TARANCHUK, V. GAVRONSKIY
Khmelnytskyi National University

GENERATION OF BROADBAND CHAOTIC SIGNALS FOR HIDDEN TRANSMISSION OF INFORMATION IN TELECOMMUNICATION SYSTEMS

The article is devoted to mathematical modelling of a broadband chaotic oscillation generator based on the classical nonlinear Lorentz dynamical system. A model of the information transmission system with chaotic masking of an arbitrary narrowband signal by a broadband chaotic signal was built on the basis of two synchronously connected Lorentz dynamic generators. The numerical solution of the system's differential equations and the amplitude spectrum of the output signal of the chaotic generator were calculated using Matlab software. In order to study the change in the dynamic regime depending on the parameters of the model, the spectrum of Lyapunov exponents was calculated and a bifurcation diagram was constructed. The model of the synchronization system of coupled dynamic systems and the model of the narrowband signal generator with any type of modulation were built in the Simulink software.

Keywords: chaos, chaotic masking, dynamic systems, synchronization.

Вступ

Однією з головних вимог, що ставиться до телекомунікаційних систем та мереж, є інформаційна захищеність. Криптографічні методи, що базуються на математичних алгоритмах, використовуються для шифрування даних з подальшою передачею їх відкритими каналами зв'язку. Додатковим ступенем захисту є приховання самого факту передачі інформації, наприклад, за допомогою методів цифрової стеганографії [1]. Іншим підходом до розв'язання цієї задачі є використання в якості носіїв інформації хаотичних сигналів, які характеризуються широким неперервним спектром та високою інформаційною ємністю [2–5]. Пристрої, побудовані на основі відносно нескладних математичних моделей, здатні генерувати неперіодичні електромагнітні коливання складної форми та дозволяють керувати хаотичними режимами за рахунок малих змін параметрів системи. Серед методів введення інформації в хаотичні сигнали, окрім модуляції параметрів нелінійної системи генератора, в науково-технічній літературі запропоновано ряд таких підходів, як хаотичне маскування (англ. chaotic masking), перемикання хаотичних режимів (англ. chaos shift keying), нелінійне підмішування (англ. nonlinear mixing) тощо [2, 6]. Таким чином, каналом зв'язку передається шумоподібний хаотичний сигнал, когерентний прийом якого здійснюється за рахунок синхронізації хаотичних систем з подальшою демодуляцією хаотичних коливань. Отже, для прийому та обробки хаотичних сигналів на приймальній стороні повинні бути повністю або частково відтворені електричні кола генератора передавача та власне динамічний режим його роботи, що можна розглядати як додатковий ступінь захисту при передачі інформації в телекомунікаційних системах.

Математична модель генератора хаотичних коливань

Розглянемо в якості математичної моделі генератора хаотичних коливань динамічну систему Лоренца, яка складається з трьох звичайних диференціальних рівнянь першого порядку:

$$\begin{cases} \dot{x} = \sigma\left(y - x\right) \\ \dot{y} = x\left(r - z\right) - y \\ \dot{z} = xy - bz \end{cases}; \quad (1)$$

де σ, r, b – дійсні додатні параметри системи.

Система Лоренца є нелінійною динамічною системою, яка при певних значеннях параметрів σ, r, b має нетривіальні розв'язки складної форми та високу чутливість до початкових умов [7, 8]. Так як праві

частини рівнянь системи (1) не містять вільних членів, то система є однорідною. В результаті заміні $x \to -x$, $y \to -y$ не змінюється вигляд рівнянь системи (1), що є свідченням симетричності системи Лоренца.

Для системи (1) дивергенція фазового потоку:

$$div(\dot{x}, \dot{y}, \dot{z}) = -\sigma - 1 - b < 0, \tag{2}$$

тоді, згідно з теоремою Ліувіля, фазовий потік стискає деякий об'єм фазового простору $V(t)$ згідно з наступним співвідношенням:

$$V(t) = V(0)e^{-(\sigma+b+1)t}, \tag{3}$$

отже, системи Лоренца є дисипативною.

Система Лоренца має нульову точку рівноваги $M_0 = (0;0;0)$ при довільних значеннях параметрів, а при $r > 1$ ще дві відмінні від нуля точки рівноваги:

$$M_{1,2} = \left(\pm\sqrt{b(r-1)}, \pm\sqrt{b(r-1)}, r-1\right). \tag{4}$$

У випадку, якщо $0 < r < 1$, єдиною точкою рівноваги, що притягує всі траєкторії у фазовому просторі, є точка M_0. При досягненні параметра значення $r = 1$ відбувається вилкоподібна біфуркація, що супроводжується (при $r > 1$) втратою стійкості точки M_0 та появою пари стійких положень рівноваги $M_{1,2}$. Точки $M_{1,2}$ є стійкими вузлами при $1 < r < 1,345$ та стійкими фокусами при $1,345 < r < 24,737$. Розмах коливань у фазовому просторі відносно положень рівноваги збільшується із зростанням параметра r. Досягнувши значення $r \approx 13,927$ спостерігається перестроювання атрактора у фазовому просторі: за нульових початкових умов, здійснивши оберт навколо однієї з точок рівноваги, траєкторія повернеться у початок координат. Далі, зі зростанням параметра r, залежно від напрямку, траєкторія приходить в одну з точок $M_{1,2}$, гомоклінічні траєкторії переходять у граничні цикли, а розмах коливань зменшується. Досягнувши значення $r \approx 24,06$ відбувається наступне перестроювання атрактора: разом із стійкими точками $M_{1,2}$ у фазовому просторі виникає складна притягаюча структура, яка відповідає хаотичному режиму системи – «дивному атрактору» Лоренца. Точки $M_{1,2}$ втрачають стійкість після досягнення значення $r = r_k$. Для значень параметрів системи $\sigma = 10$ та $b = 8/3$, значення $r_k \approx 24,74$.

В загальному випадку значення параметра r_k при заданих σ та b визначається співвідношенням:

$$r_k = \frac{\sigma(\sigma + b + 3)}{\sigma - b - 1}. \tag{5}$$

На рис. 1 показані характерні траєкторії системи (1) при різних значеннях параметра r для двох наборів початкових умов: I_1 (0,1; 1; 1) та I_2 (–0,1; –1; 1).

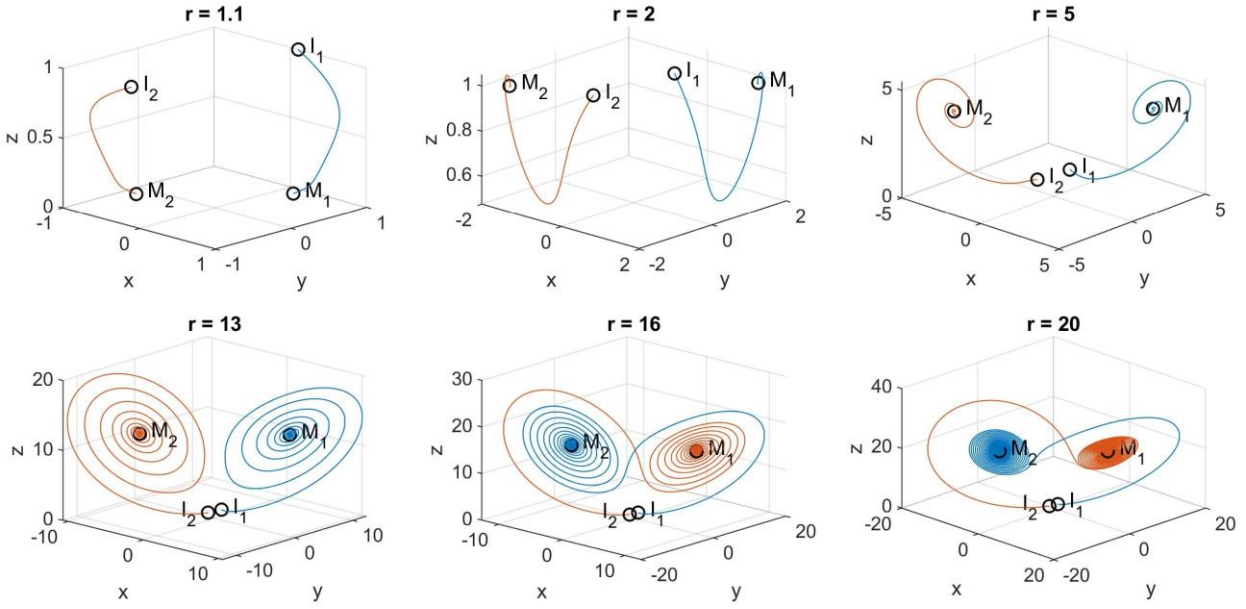
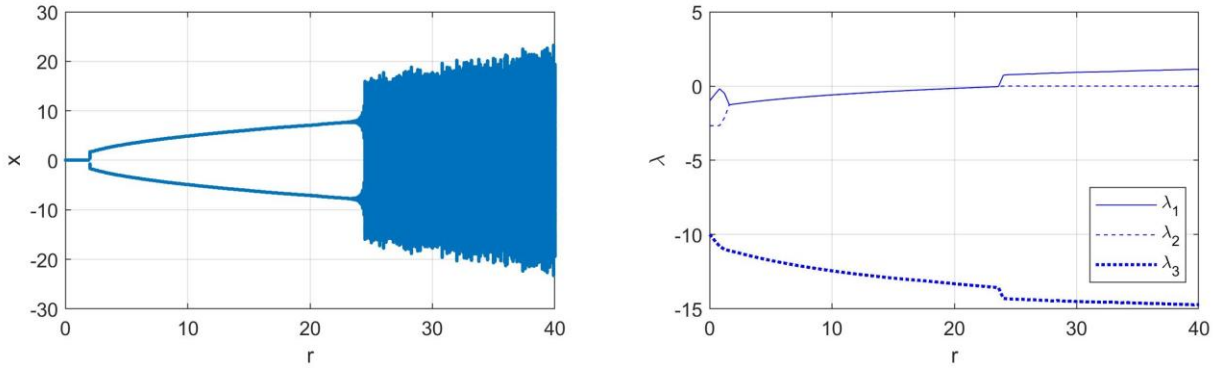


Рис. 1. Фазові траєкторії системи Лоренца для різних значеннях параметра *r*

Зміну динамічного режиму системи Лоренца за координатою x при зміні параметра $r \in [0{,}1;\ 40]$ ілюструє біфуркаційна діаграма, зображена на рис. 2, а.



а б

Рис. 2. Зміна динамічного режиму та ступеня хаотичності системи Лоренца залежно від параметра *r*: біфуркаційна діаграма (а), спектр показників Ляпунова (б)

Для кількісної оцінки хаотичності системи були розраховані показники Ляпунова [9, 10] λ_k, $k = 1..3$, для різних значеннях параметра $r \in [0{,}1;\ 40]$. Спектр показників Ляпунова для вказаного діапазону значень параметра r зображено на рис. 2, б.

При значеннях параметрів $\sigma = 10$, $b = 8/3$, починаючи із значення $r \approx 24{,}74$, система Лоренца генерує хаотичні коливання, про що свідчить форма біфуркаційної діаграми [11] (рис. 2, а) та додатній знак старшого показника Ляпунова (рис. 2, б).

В якості набору параметрів, за яких система (1) демонструє хаотичну поведінку, було прийнято: $\sigma = 10$, $r = 35$, $b = 8/3$. Фазовий портрет атрактора, форму широкосмугового сигналу та його амплітудний спектр показано на рис. 3.

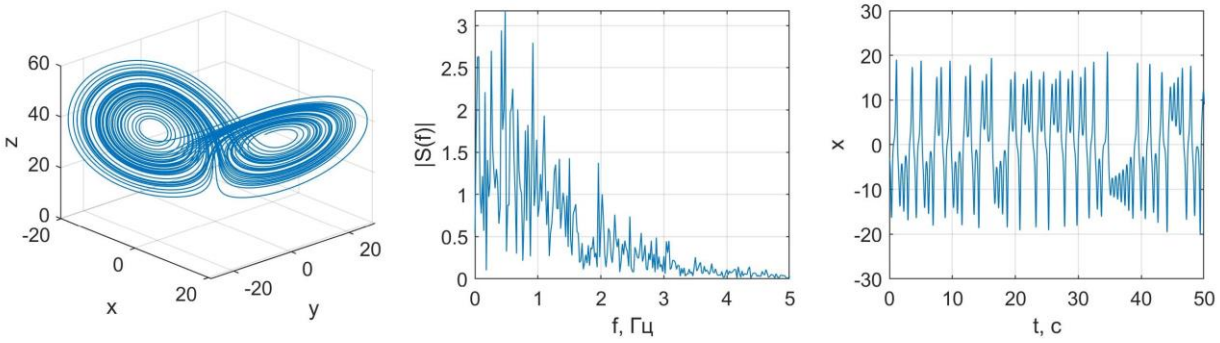
У хаотичному режимі система Лоренца генерує широкосмугові сигнали складної форми із неперервним спектром та високими кореляційними та ортогональними властивостями [8]. Висока інформаційна ємність та сильна залежність від початкових умов обумовлює використання сигналів такого типу в системах прихованої передачі інформації з шифруванням даних.

Синхронізація зв'язаних динамічних систем та маскування вузькосмугового сигналу широкосмуговим хаотичним сигналом

Головною проблемою, яку необхідно вирішити для ефективного використання хаотичних сигналів для передачі інформації в телекомунікаційних системах є задача синхронізація хаотичних генераторів на передавальній та приймальній сторонах – «ведучої» та «веденої» систем відповідно (див. рис. 4, б).

Розглянемо пару зв'язаних систем Лоренца з однаковими значеннями параметрів σ, r та b, що описується наступною системою рівнянь:

$$\begin{cases} \dot{x}_1 = \sigma(y_1 - x_1) \\ \dot{y}_1 = x_1(r - z_1) - y_1 \\ \dot{z}_1 = x_1 y_1 - b z_1 \\ \dot{x}_2 = \sigma(y_2 - x_2) \\ \dot{y}_2 = x_2(r - z_2) - y_2 \\ \dot{z}_2 = x_2 y_2 - b z_2 \end{cases} \quad (6)$$



а б в

Рис. 3. Хаотичний режим системи Лоренца для набору параметрів σ = 10, *r* = 35, *b* = 8/3: атрактор у фазовому просторі – а), амплітудний спектр сигналу координати *x* – б), часовий графік сигналу *x*

Синхронізація цих двох систем можлива якщо існують фазові траєкторії $\mathbf{U}_1$ та $\mathbf{U}_2$ такі, що при $t \to \infty$ відстань між траєкторіями $\delta \to 0$, тобто:

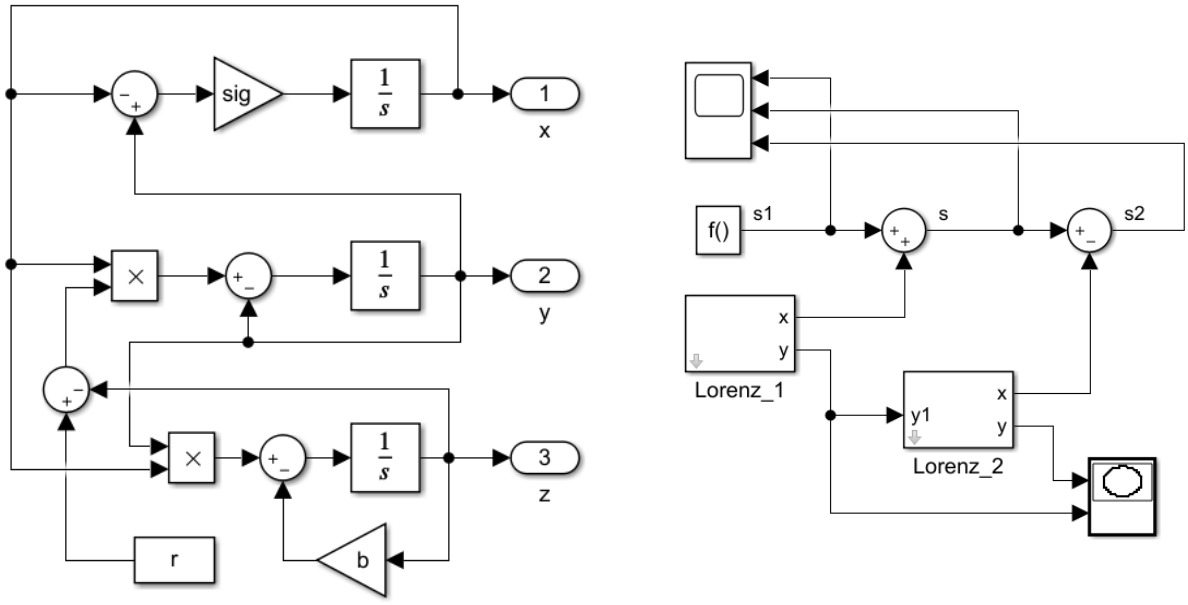
$$\lim_{t\to\infty} \mathbf{U}_2 = \mathbf{U}_1 \tag{7}$$

Крім того, рух системи (6) цією траєкторією повинен бути стійким по відношенню до завад. Необхідною умовою цього є від'ємне значення старшого показника Ляпунова «веденої» системи [7]. Моделювання процесу синхронізації зв'язаних систем Лоренца було виконано засобами MATLAB/Simulink.

Комп'ютерна Simulink-модель, що складається з трьох інтеграторів, які призначені для чисельного розв'язку динамічної системи Лоренца (1), зображена на рис. 4, а. Вихідними сигналами системи є часові значення координат *x*, *y*, *z*.

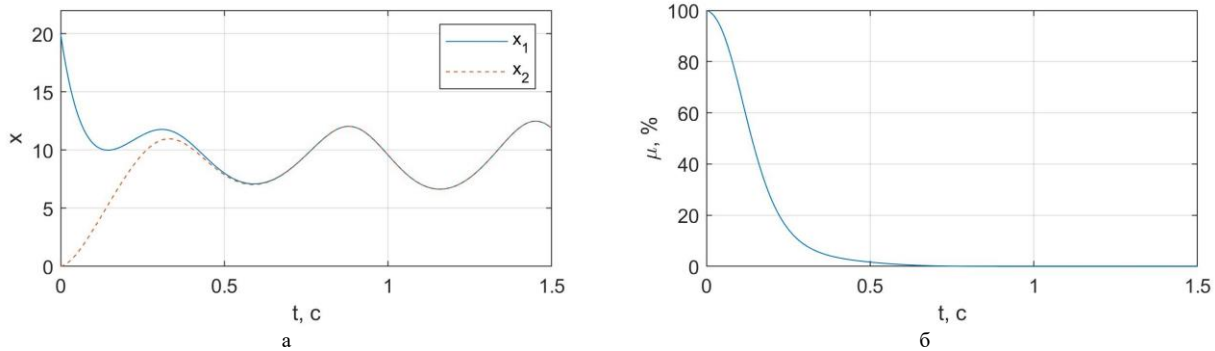
Система синхронізації двох зв'язаних систем Лоренца, *Lorenz_1* та *Lorenz_2*, показана на рис. 4, б. Для реалізації синхронного відгуку системи *Lorenz_2* використовується сигнал *y* «ведучої» системи *Lorenz_1*, а сигнал *x* слугує носієм інформаційного сигналу s_1.

Перехідний процес синхронізації динамічних систем Лоренца для сигналу *x* показано на рис. 5, а. На рис. 5, б зображено графік відносної похибки синхронізації μ.



а б

Рис. 4. Simulink-модель динамічної системи Лоренца (а) та системи синхронізації двох зв'язаних систем Лоренца з хаотичним маскуванням інформаційного сигналу (б)



а б

Рис. 5. Процес синхронізації зв'язаних динамічних систем Лоренца: часові діаграми вихідних сигналів x_1 та x_2 зв'язаних систем (а), відносна похибка синхронізації (б)

Представимо довільний вузькосмуговий сигнал у вигляді:

$$s\left[u(t),t\right] = S\left[u(t),t\right]\cdot\sin\left(\omega_0 t + \Psi\left[u(t),t\right]\right), \tag{8}$$

де $S\left[u(t),t\right]$ – амплітуда сигналу,

$\Psi\left[u(t),t\right] = \Phi\left[u(t),t\right] + \varphi_0$ – повна фаза сигналу.

Нехай $u(t)$ – повільно зростаючою функцією часу, тоді при диференціюванні вважатимемо $u(t) = u = \text{const}$.

Продиференціювавши вираз (8) двічі по часу, ввівши заміни $\sin\Psi = s/S$ та $\cos\Psi = \left(\dot{s} - \dot{S}\,s/S\right)\Big/S\dot{\Psi}$, отримаємо лінійне диференціальне рівняння зі змінними коефіцієнтами:

$$\ddot{s} - \left[\frac{\ddot{\Psi}}{\dot{\Psi}} + \frac{2\dot{S}}{S}\right]\dot{s} + \left[\dot{\Psi}^2 + \frac{1}{S}\left(\frac{2\dot{S}^2}{S} + \frac{\dot{S}\ddot{\Psi}}{\dot{\Psi}} - \ddot{S}\right)\right]s = 0\,. \tag{9}$$

Форма сигналу $s(t)$, який є розв'язкам рівняння (9), залежить від типу модуляції, яка в свою чергу, в рамках описуваної моделі, задається законом зміни амплітуди $S\left[u(t),t\right]$ та повної фази $\Psi\left[u(t),t\right]$.

Наприклад, для сигналу з частотною модуляцією (ЧМ):

$$S\left[u(t),t\right] = S_0 = \text{const}\,, \tag{10}$$

$$\Psi\left[u(t),t\right] = \omega_0 t + m_{чм}\int_0^t u(t)\,dt + \varphi_0\,, \tag{11}$$

де ω_0 – частота несучого коливання; $m_{чм}$ – індекс модуляції; φ_0 – початкова фаза.

Комп'ютерна Simulink-модель генератора вузькосмугових сигналів, побудована згідно рівняння (9) представлена на рис. 6. Вхідними сигналами для моделі є амплітуда S та повна фаза Ψ.

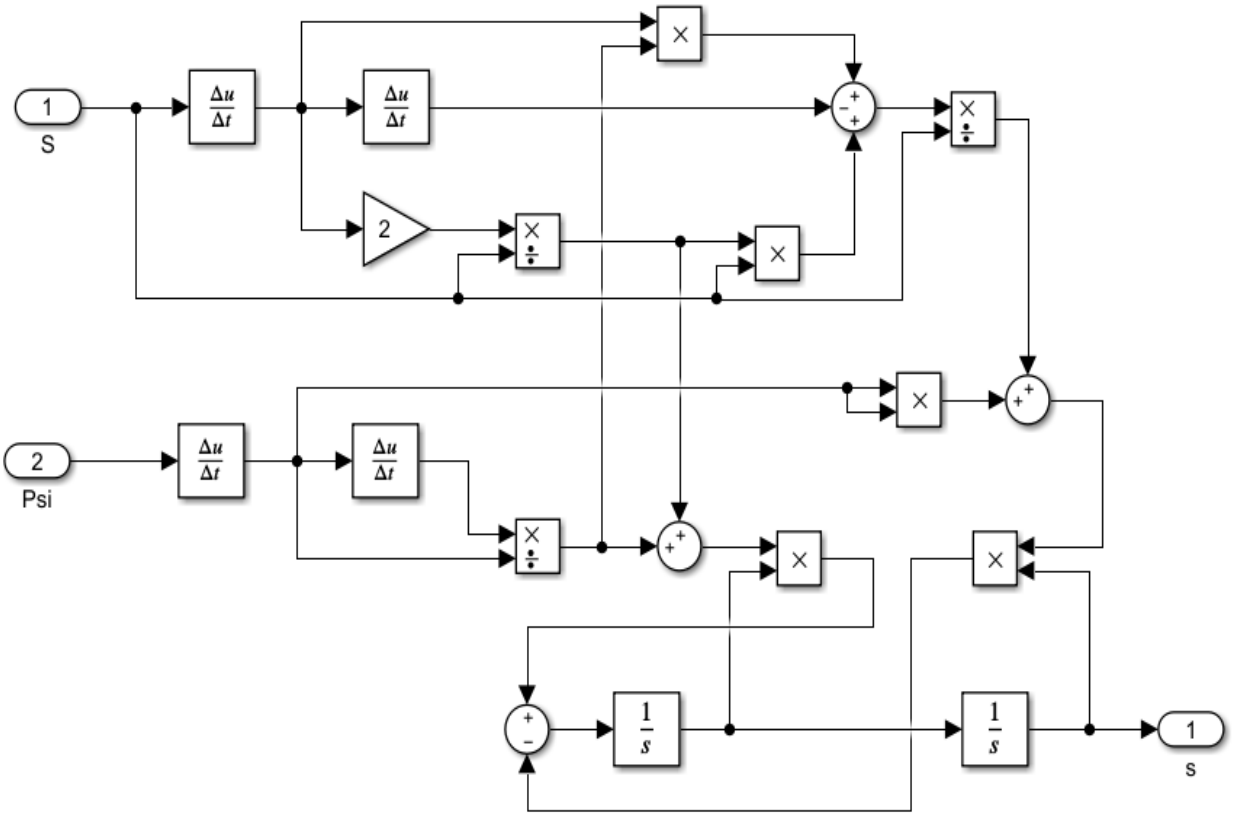


Рис. 6. Simulink-модель генератора вузькосмугових сигналів із заданою формою амплітуди та фази

Часові залежності та амплітудні спектри вихідних сигналів систем передачі та прийому, а також сигналу в каналі зв'язку, показано на рис. 7.

Тестовий ЧМ-сигнал s_1, отриманий на виході моделі, показаної на рис. 6, адитивно підмішується до вихідного хаотичного сигналу x_1 системи *Lorenz_1* (рис. 4, б) та разом із сигналом синхронізації y передається каналом зв'язку (рис. 7, б).

На приймальній стороні тестовий сигнал виділяється шляхом віднімання від прийнятого хаотичного сигналу s сигналу x_2, згенерованого системою *Lorenz_2* (рис. 4, б), що синхронізується сигналом y. Після завершення перехідного процесу, після встановлення режиму синхронізації, виділений сигнал s_2 (рис. 7, е) співпадає з оригінальним сигналом повідомлення s_1 (рис. 7, а). Параметри систем *Lorenz_1* та *Lorenz_2* вважаються ідентичними, а канал зв'язку – ідеальним.

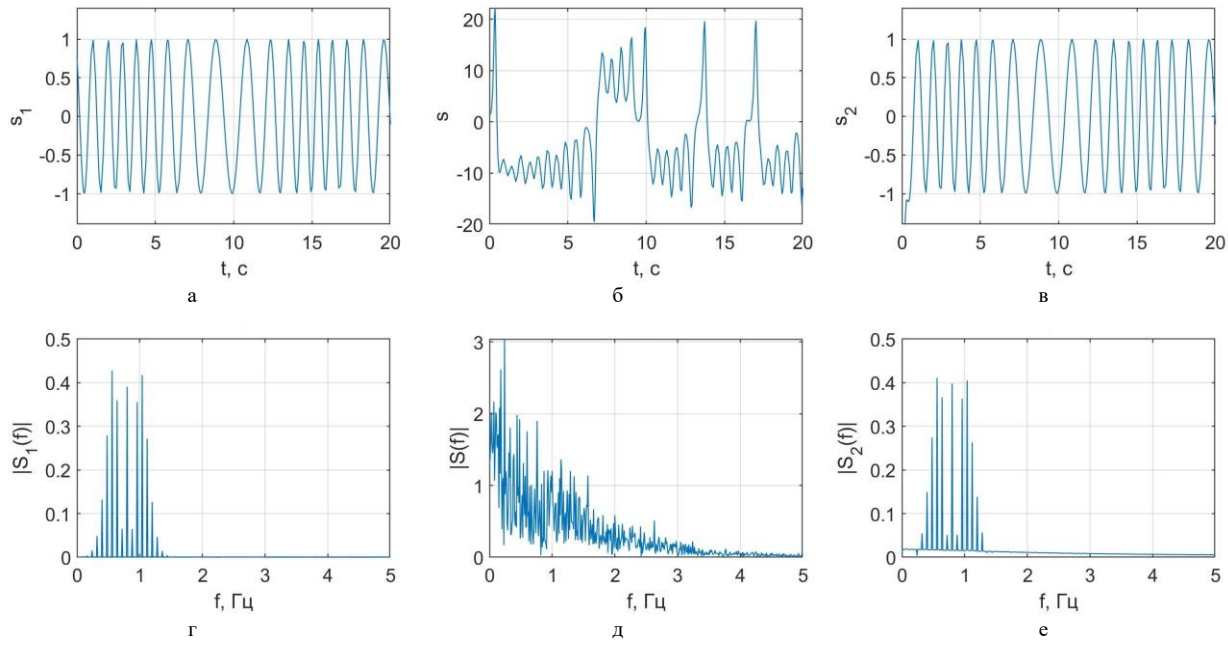


Рис. 7. Хаотичне маскування тестового вузькосмугового ЧМ-сигналу:
сигнал на вході системи передачі та його амплітудний спектр – а), г);
сигнал, переданий каналом зв'язку та його спектр – б), д);
сигнал на виході приймальної системи та його спектр – в), е)

Висновки

1. Перспектива використання пристроїв із хаотичної динамікою в сучасних засобах телекомунікації обумовлена рядом факторів, серед яких висока інформаційна ємність, широкий спектр частот та конфіденційність передачі повідомлень. Можливість реалізації на базі одного пристрою великої кількості хаотичних режимів в перспективі дає можливість побудови багатоканальних систем передачі інформації. Сильна залежність від початкових умов та нестійкість фазових траєкторій дозволяє за рахунок малих впливів керувати динамікою хаотичних генераторів та здійснювати модуляцію з великою швидкістю.

2. Не дивлячись на простоту реалізації, метод хаотичного маскування має ряд суттєвих недоліків. Так, при наявності завад в каналі зв'язку інформаційний сигнал, потужність якого апріорі є нижчою порівняно із несучим хаотичним сигналом, стає співрозмірним із шумами каналу. Збільшення рівня інформаційного сигналу призводить до втрати конфіденційності, оскільки можливим стає несанкціонований перехват інформаційного повідомлення шляхом відфільтровування хаотичної складової. Таким чином, в ході проектування системи передачі, основаній на хаотичному маскуванні, необхідно визначити оптимальне співвідношення сигнал/хаос виходячи із оцінки можливого рівня шумів в каналі та потрібної якості передачі.

3. Описаний підхід може бути застосований для багатоканальної передачі вузькосмугових сигналів з кутовою модуляцією, наприклад, в безпровідних інфокомунікаційних системах з використанням кварцових сенсорів фізичних параметрів з модульованим міжелектродним зазором збудження п'єзорезонатора [12].

Література

1. Абазина Е.С. Цифровая стеганография: состояние и перспективы / Е.С. Абазина, А.А. Ерунов // Системы управления, связи и безопасности. – 2016. – № 2. – С. 182–201.

2. Земляный О.В. Передача информации на основе манипуляции спектром широкополосного хаотического сигнала / О. В. Земляный // Радиофизика и электроника. – 2015. – Т. 6(20), № 3. – С. 72–78.

3. Иванюк П.В. Хаотическое маскирование информационных сигналов с использованием генератора на базе системы Лю / П.В. Иванюк, Л.Ф. Политанский, Р.Л. Политанский, О.М. Элияшив // Технология и конструирование в электронной аппаратуре. – 2012. – № 3. – С. 11–17.

4. Пятін І.С. Конфіденційна система зв'язку / І.С. Пятін, В.І. Лужанський, Л.В. Карпова // Вісник Хмельницького національного університету. Технічні науки. – 2015. – № 1. – С. 207–212.

5. Колесов В.В. Применение дискретных хаотических алгоритмов в широкополосных телекоммуникационных системах / В.В. Колесов, А.И. Полубехин, Е.П. Чигин, А.Д. Юрин // Вестник СибГУТИ. – 2016. – № 3. – С. 77–92.

6. Агуреев К.И. Применение детерминированного хаоса для передачи информации / К.И. Агуреев // Известия ТулГУ. Технические науки. – 2014. – Вып. 11. Ч. 2. – С. 197–212.

7. Дмитриев А.С. Динамический хаос: новые носители информации для систем связи / А.С. Дмитриев, А.И. Панас. – М. : Изд-во Физико-математической литературы, 2002. – 252 с.

8. Прикладне застосування теорії хаотичних систем у телекомунікаціях : монографія / [Ю.Я. Бобало, С.Д. Галюк, М.М. Климаш, Р.Л. Політанський] ; Нац. ун-т «Львів. політехніка». – Львів : Коло, 2015. – 178 с.

9. Передерий Ю.А. Метод оценки спектра ляпуновских показателей по временной реализации / Ю.А. Передерий // Известия вузов. ПНД. – 2012. – Т. 20, вып. 1. – С. 99–104.

10. M.-F. Danca. Matlab code for Lyapunov exponents of fractional order systems / Marius-F. Danca, N.V. Kuznetsov // International Journal of Bifurcation and Chaos. – 2018. – Vol. 28, No. 05, 1850067. – 14 p.

11. Kehui Sun. Bifurcations of fractional-order diffusionless Lorenz system / Kehui Sun, Xia Wang, J.C. Sprott // International Journal of Bifurcation and Chaos. – 2010. – Vol. 20, No. 04. – P. 1209–1219.

12. Taranchuk A.A. Construction of measuring piezoresonance mechanotrons and their practical implementation for telemedicine diagnostic systems / A.A. Taranchuk // Telecommunications and Radio Engineering. – 2018. – Volume 77, Issue 3. – P. 269–281.

References

1. Abazina E. S. Digital Steganography: Status and Development Outlook / E. S. Abazina, A. A. Erunov // Systems of Control, Communication and Security. – 2016. – Issue 2. – P. 182–201.

2. Zemlyaniy O.V. Information transmission based on spectrum manipulation of a wideband chaotic signal / O.V. Zemlyaniy // Radio physics and electronics. – 2015. – Volume 6(20), Issue 3. – P. 72–78.

3. Ivanyuk P.V. Chaotic masking of information signals using generator based on the Liu system / P.V. Ivanyuk, L.F. Politansky, R.L. Politansky, O.M. Eliiashyv // Tekhnologiya i Konstruirovanie v Elektronnoi Apparature. – 2012. – Issue 3. – P. 11–17.

4. Pyatin I.S. Confidential communications system / I.S. Pyatin, V.I. Lughanskiy, L.V. Karpova // Herald of Khmelnytskyi National Universityu. Technical sciences. – 2015. – Volume 221. Issue 1. – P. 207–212.

5. Kolesov V.V. Application of discrete chaotic algorithms in broadband telecommunication systems / Vladimir V. Kolesov, Alexander I. Polubekhin, Eugene P. Chigin, Alexander D. Yurin // Vestnik SibGUTI. – 2016. – Issue 3. – P. 77–92.

6. Agureev K.I. The application of deterministic chaos to transmisson of information (review) / K.I. Agureev // Izvestiya TulGU. Technical sciences. – 2014. – Issue. 11. Part. 2. – P.197–212.

7. Dmitriev A.S. Dynamic chaos: novel type of information carrier for communication systems / A.S. Dmitriev, A.I. Panas. – M. : Izdatelstvo Fizikomatematicheskoy literatury, 2002. – 252 p.

8. Prikladne zastosuvannya teorii khaotichnikh sistem u telekomunikacziyakh: monografiya / [Yu.Ya. Bobalo, S.D. Galyuk, M.M. Klimash, R.L. Politansky] ; Nacz. un-t «Lviv. politekhnika». – Lviv : Kolo, 2015. – 178 p.

9. Perederiy Y.A. Method for calculation of Lyapunov exponents spectrum from data series / Y.A. Perederiy // Izvestiya VUZ. AND. – 2012. – Volume 20, Issue 1. – P. 99–104.

10. Danca M.-F. Matlab code for Lyapunov exponents of fractional order systems / Marius-F. Danca, N.V. Kuznetsov // International Journal of Bifurcation and Chaos. – 2018. – Volume 28, Issue 05, 1850067. – 14 p.

11. Kehui Sun. Bifurcations of fractional-order diffusionless Lorenz system / Kehui Sun, Xia Wang, J.C. Sprott // International Journal of Bifurcation and Chaos. – 2010. – Volume 20, Issue 04. – P. 1209–1219.

12. Taranchuk A.A. Construction of measuring piezoresonance mechanotrons and their practical implementation for telemedicine diagnostic systems / A.A. Taranchuk // Telecommunications and Radio Engineering. – 2018. – Volume 77, Issue 3. – P. 269–281.

Рецензія/Peer review : 19.10.2020 р. Надрукована/Printed :06.11.2020 р.