UDC 621.391

CHARACTERISTICS IMPROVEMENT OF THE WIDEBAND TELECOMMUNICATION SYSTEM APPLYING CHAOS BASED PSEUDORANDOM SEQUENCE

Semenko A.I.
Kyiv, Ukraine
Kushnir M. Ya.
Physical, technical and computer science institute Chernivtsi National University
Chernivtsi, Ukraine
Bokla N.I.
Department of Automated design National University of Lviv Polytechnic Lviv, Ukraine
Shestopal Y.O.
Department of Telecommunication systems State University of Telecommunications
Kyiv, Ukraine

Background. Telecommunication systems with a broadband signal have undoubted advantages: increased noise immunity with narrowband and wideband interference, confidentiality of information transmission, as well as improved electromagnetic compatibility with neighboring radio-electronic devices.

A broadband signal is usually formed by direct spread spectrum using well-known classical pseudo-random sequences (PRS): m-sequences, Kasami, Gold, Walsh sequences, which can be decoded and received at the receiver.

Objective. The aim of the paper is creating PRS on the basis of chaos, which the subscriber is practically unable to decode, and thus ensure increased confidentiality of information transmission.

Methods. Using the mathematical model of chaotic logistic mapping, which, as shown by preliminary studies, provides the best results, as well as referring to the bifurcation diagram of Feigenbaum, the parameters of 3-secret keys are defined and the PRS of the selected length is created. Based on the application of the graphical user interface developed in the MATLAB system, a correlation analysis of the resulting PRS is performed and the PRS is determined with the minimum side lobes of the autocorrelation function.

Results. By empirical decision of 3 secret keys of the dynamic parameter of the Feigenbaum diagram, the initial value of the sequence and the number of the initial pulse of the PRS, as well as the study of the autocorrelation function, we obtained a PRS with a side lobe level of the autocorrelation function acceptable for practical use of no more than 0.25.

Conclusions. The use of well-known pseudo-random sequence: Walsh's, Kasami's, Gold's, creating a system with a noise-like signal doesn't ensure complete confidentiality of information transmission, since they can be decoded.

The most acceptable by the criterion of the side lobe minimum of the autocorrelation function – no worse than 0.25 – is the use of chaos based on the Feigenbaum logistic map.

When creating pseudo-random sequences based on chaos, the best results are obtained by choosing the maximum value of the dynamic parameter of the Feigenbaum diagram at the level of the boundary value equal to 4, with an accuracy of 0.05.

Keywords: telecommunication system; broadband pseudo-noise signal; logistic mapping; signal base; radio channel.

1. Introduction

Currently, special attention is paid to telecommunication systems (TCS) with a broadband signal, with enhanced noise immunity for both narrowband and wideband interference, improved confidentiality of information transmission, as well as electromagnetic compatibility with neighboring electronic devices [1,2].

The main characteristic of a broadband signal is the signal base

$$B = TW \quad , \qquad (1)$$

where T is the duration of the signal, W is the width of the signal spectrum.

For the broadband signal $B \gg 1$.

2. Advantages of telecommunication systems with broadband signal

All TCSs are affected by both internal Gaussian thermal noise and external interference.

Near the transmitter, signal spectrum width of which $W_п$ «W, TCS can be affected by narrowband interference. The ratio of the signal power to the total noise power and interference at the outputs of the matched filter will be [2]

$$\gamma = 2E / (N_0 + P_i / W), \qquad (2)$$

where E is the energy of the bit, N_0 is the spectral density of thermal noise, P_i is the interference power.

Obviously, regardless of the particular interference band W_i, the signal / (noise + interference) ratio at the output of the matched

filter behaves as if the interference power were evenly distributed in the signal band W, adding to the noise an additional noise with a spectral density P_i / W, and the total noise has the properties of Gaussian noise [2].

It is possible to neutralize the effect of narrow-band interference by using a notch filter that "cuts" the interference from the signal spectrum.

Then, at the output of the matched filter, we obtain the signal / (noise + interference)

$$\gamma_1 = \gamma_2 (1 - W_i / W), \quad (3)$$

where γ_2 is the actual signal-to-noise ratio at the output of the matched filter in the absence of interference.

Obviously, the greater the width of the signal spectrum compared to the width of the interference spectrum, the less the influence of narrowband interference on the operation of the system.

The attainment of high noise immunity of TCS with narrowband interference (without using the brute force method by means of transmitter power increase) is possible only by expanding the signal spectrum as much as possible.

As a deliberate counteraction to the operation of the TCS when a signal is detected, a barrier noise can be used with spectrum width exceeding the signal spectrum width. In this case, the signal / (noise + interference) ratio will also be determined by the formula (2).

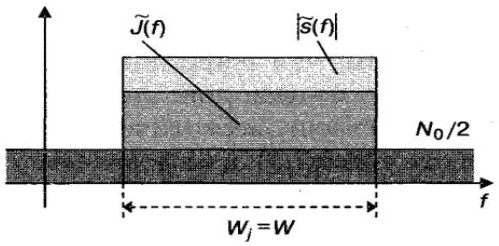

Fig.1.The spectrum of the signal, obstruction and noise:
j (f) is the spectral power density of the interference; s(f) is the spectral power density of the signal

It's obvious that the only way to increase the immunity of the system to blocking interference is to use an ultra-wideband signal with a base $B \gg 1$.

In the case of electronic countermeasures, effective interference can be organized only when a signal is detected in the air with the definition of the frequency and width of the spectrum. A system with a broadband signal should work as secretively as possible with a minimum spectral density of the signal, using special modulation techniques. The latter should carry out a supersensitive energy reception of the signal in the mode of the radiometer in a wide frequency band.

Obviously, the larger the base of the broadband signal, the more difficult it will be to detect the system to the interference provider. Widening of the signal spectrum reduces its spectral density, masking it under noise.

A characteristic feature of electromagnetic compatibility of systems is their conflict-free coexistence in a given region. For this system transmitters must emit a minimum signal in the receiver frequency band to ensure that the spectral density of the signal is less than a certain threshold level, for example, -7 dB from the noise level. It is this ability that creates a broadband signal.

The broadband signal provides high resolution when receiving short pulses of duration Δt

$$\Delta t = 1 / W. \quad (4)$$

With multipath propagation of the signal it allows identifying short pulses of signals, with a delay coming to the input of the receiver. Such pulses are processed in the equalizer or rake receiver, thereby creating a sum signal that exceeds the signal-to-noise ratio at the receiver output.

A wideband signal is usually formed by direct spectrum spread with the use of a number of known pseudo-random modulated sequences (PRS): m-sequences, Kasami, Gold's sequences, etc., as well as Walsh code.

The main requirement in choosing the type of PRS is obtaining minimum side lobes of the autocorrelation function for single-channel systems and also minimum petals of the mutually correlating functions for multichannel systems.

The interceptor can unravel the structure of the signal with a simple enumeration method (brute force method) using a bank of parallel matching filters or filters that are rearranged in series if the signal is received for a long time. Therefore, systems using known pseudo-random sequences can't be considered to be protected against unauthorized access.

3. Using a chaos to create PRS

At present methods have been developed for obtaining a sequence of bits with alternating symbols + 1, -1 from chaos, the random character of which makes it possible to obtain pseudo-random sequences of large length [6]. Any analysis of these sequences does not make it possible to reproduce them and they can't be used to intercept the signal, therefore they have unique advantages when used for spreading the signal spectrum and creating a pseudo noise broadband signal.

As shown in [7,8] the best results for the criterion of the minimum level of the maximum side lobes of ACP PRS are obtained on the basis of chaotic logistic mapping, which has a mathematical model

$$x_{n+1} = rx_n\left(1-x_n\right), \qquad (5)$$

where x_n is the value of the system variables at the step n, and r is the parameter of the dynamic system.

The initial states of the system are set by values $x_0 \in (0 \div 1)$. The values of the parameter r for the Feigenbaum parabola are within the limits $\left(3,57 \div 4\right]$ (Fig. 2), that guarantees the chaotic state of the system and the initial sequences will have a high level of randomness.

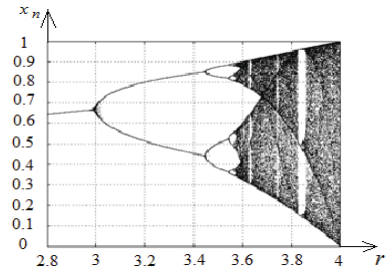

Fig. 2. The bifurcation diagram of Feigenbaum's logistic mapping

Using the diagram of Fig. 2 it is possible to determine the value of the parameter r at which the developed chaos is realized. In our calculations, it assumed a value of $3.9 < r < 4.0$. Other encryption keys will be the initial value of x_0 and the value of n_k, from which we begin to form the PRS.

On the basis of chaos with logistic reflection, 10 sequences of 200 pulses in length are obtained according to the parameters shown in Table 1.

The first sequence with the number of pulses 200 has the form

-11-11-11-1-1-11-1-1-11-11-1-11-1-1111-1-11-1-1111-1-111-11-111-11-11-11 -11-1

-11-111-1111111111-11-1-111-11-1-11-11-111-11-1-1-11-11-1-1-1111-1-11-1-1

-111-1-11-111-1-11-1-1-11-11-1-1-111-11-11-1-1111-1-11-11-11-1-111-11-11 -1-11

11-111-11-111-111-11-1-1-11-11-1-1-111-1-11-111-11-1-1-11-1-1-11-11-11- 11-1-1.

In Table 1 the minimum values of the maximum level of the side lobes of the auto-correlation function obtained from the results of studies of the obtained sequences using the graphical interface method [9].

TABLE 1. ACF PRS from chaos based on logistic mapping

№ impuls. / №PRS (x_0)	10	20	30	40	50	100	150	200
1 (0,1)	0,6; -0,6	0,4; -0,4	0,4; -0,4	0,5	-0,4	-0,3	-0,3	-0,3
2 (0,2)	0,2; -0,2	0,5; -0,5	-0,5	0,4; -0,4	0,3; -0,3	0,2; -0,2	0,2; -0,2	0,2; -0,2
3 (0,3)	0,6	0,4	0,4	0,3	0,3	0,2; -0,2	0,2; -0,2	0,2; -0,2
4 (0,4)	0,6	0,4; -0,4	0,4; -0,4	0,4	-0,3	-0,3	0,2; -0,2	-0,3
5 (0,05)	-0,6	0,2; -0,2	-0,4	0,4	0,3; -0,3	0,2	0,2; -0,2	0,2, -0,2
6 (0,5)	0,6	-0,4	-0,3	-0,3	0,3	0,2; -0,2	0,2; -0,2	0,2; -0,2
7 (0,6)	0,6	0,4; -0,4	0,4; -0,4	-0,3	-0,3	-0,4	0,2; -0,2	-0,3
8 (0,7)	0,6	0,4	0,4; -0,4	0,3	0,4	0,2; -0,2	0,2; -0,2	0,2; -0,2
9 (0,8)	0,2; -0,2	0,4; -0,4	-0,5	0,4; -0,4	0,4	0,2; -0,2	0,3	0,2; -0,2
10 (0,9)	0,6; -0,6	0,4; -0,4	0,4; -0,4	0,4; -0,4	-0,4	-0,3	-0,3	-0,3

Note: When creating all implementations, the parameters used are: r = 3.89; q = 0.55

4. Construction of TSS using the PRS based on chaos

In a number of cases it is important to create a single-channel TCS with a broadband pseudo-noise signal, which has the advantages listed above, which are already manifested when the base is B = 10-20 dB [2].

Fig. 3 shows a scheme for constructing a single-channel practical TCS using a pseudo-noise signal obtained using a chaotic-based PRS.

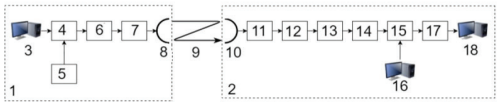

Fig.3. System construction diagram:
1 - transmitter; 2 - receiver; 3-PC for signal conditioning; 4-modulator; 5-signal generator of intermediate frequency; 6-frequency converter; 7-power amplifier; 8,10-antenna transmitter and receiver; 9-radio channel; low-noise amplifier; 12 - frequency converter; 13 - RACE - receiver; 14-demodulator; 15-correlator; 16-PC for the formation of a reference signal; 17-solving device; 18-PC for the formation the received signal.

When designing the system, the initial parameters are the available frequency resource Δf, which determines the bandwidth of the radio channel, as well as the transmission rate of information transmission (the duration of the information signal T). The use of these parameters

is determined by the base of the pseudo-noise signal

$$B = \Delta f\, T = T / \tau, \quad (6)$$

where τ is the duration of an elementary pulse of a complex signal.

It is important that the signal base is not less than 10 dB, which will provide the advantages that are characteristic for broadband systems.

Next, a pseudo-random sequence based on chaos of length N = B is determined. By using the graphical user interface method the best implementation with ACF lateral lobes of not more than 0.3 is selected.

Considering the determining value of the maximum signal base to ensure unconditional advantages of TCS with broadband noise-like signal, it is expedient to select the maximum value of the signal base.

In such a system the SNR at the receiver input should be less than the Shannon limit of -1.6 dB [2], when the signal reception is impossible. Such a system will be safe to ensure electromagnetic compatibility with nearby electronic devices, even when the signal spectrum of the system will occupy part of the band of the radio channel in which these devices operate. To do this, the broadband signal base must be at least

$$B_1 > \frac{U^2 T}{1{,}38\, No}, \quad (7)$$

where U is the bit amplitude at the receiver input, N_0 is the noise spectral density at the receiver input.

Then, a pseudo-random sequence is determined from chaos with a length of N = B. At the same time, using the method of a graphical user interface, the best implementation is chosen that has side lobes ACF of not more than 0.3

5. Conclusions

1. The use of known pseudo-random sequences - Walsh, Kasami, Gold, when creating systems with a noise-like signal does not ensure complete confidentiality of information transmission, since they can be picked up in the receiver (brute force method).
2. When a pseudo-random sequence is created, the use of chaos based on the Feigenbaum logistic map is the most acceptable by the criterion of the side lobe minimum of the autocorrelation function - not worse than 0.3.
3. Pseudo-random sequences based on chaos significantly increase the confidentiality of information transmission in systems with a noise-like signal created with their use, since no analysis of them practically allows them to be determined in the transceiver.
4. The use of pseudo-random sequences based on chaos is effective when creating telecommunication wireless systems with increased confidentiality of information transmission - radio relay, satellite and other systems, in which the possibility of taking information by unauthorized subscribers is almost completely excluded.
5. When designing the system the initial parameters are the available frequency resource, which determines the bandwidth of the radio channel, as well as the information transfer rate (the duration of the information signal) from which the broadband signal base is determined (which should be at least 10 dB), and the duration of the elementary pulse.
6. When selecting a signal base providing a signal-to-noise ratio at the input of the receiver is less than the Shannon limit (-1.6 dB), the system will be safe for electromagnetic compatibility with a number of electronic devices operating, even if the signal spectrum will occupy part of the channel in which these device.

REFERENCES

1. Varakin L.E. Communication systems with noise like signals. M.: Radio and communication, 1985. - 384 p. (In Russian)
2. Sklar B. Digital communications. Fundamentals and Applications. Edition.2,: Translation from English. – M.: Publishing House Ltd «Williams», 2004. – 1104 p. (In Russian)
3. Yu.M. Boiko and R.O. Boryachok. “Improving effectiveness for processing signals in data transmission channels with phase manipulation”, in 2013 23rd International Crimean Conference Microwave and Telecommunication Technology (CriMiCo), CriMiCo, 2013, pp. 262-263.
4. Oleg Shynkaruk, Juliy Boiko and Oleksander Eromenko. “Measurements of the energy gin in the modified circuit signal processing unit”, in 2016 13th International Conference on Modern Problems of Radio Engineering. Telecommunications and Computer Science (TCSET), 2016, pp. 582-584.
5. Ipatov V.P. Broadband systems and code channels division of the signals. M.: Technospera.2007.488 p. (In Russian)
6. Bobalo, U.Y. Practical use of the chaos systems theory in telecommunications: monograph/ U. Y. Bobalo, S. D. Galiuk, M. M. Klimash, R.L. Politanskiy. – Drogobuch – Lviv: Kolo, 2015. – 184 p. (In Ukrainian)
7. Anatolii Semenko Creation of pseudo-random sequences based on chaos for forming of wideband signal /Anatolii Semenko, Nikolai Kushnir, Nataliya Bokla, Grigoriy Kosovan// Information and Telecommunication Sciences, 2017, Volume 9, Number 2, pp 5-10.
8. Semenko A.. *Kushnir N. Bokla N. Kosovan G.* Features of creating based on chaos pseudo-random sequences**.** Modern Problems of Radio Enginiring,Telecommunications, and Computer Sciens. Proceedings of the XIIth International Conference TCSET’ 2018. Lviv-Slavsco,Ukraine.February 20-24 , 2018.Pp338-342.
9. Bokla N.I. Research of the PRS correlation properties based on gold code using Mathlab by //Vistnuk DUIKT.-2011.-Vol.9. - №4.-pp.386-391

Семенко А.І., Кушнір М.Я., Бокла Н.І., Шестопал Ю.О.

Застосування псевдовипадкової последвательности на основі хаосу для створення широкосмугових телекомунікаційних системи з поліпшеними характеристиками

Проблематика. Телекомунікаційні системи з широкосмуговим сигналом мають безперечні переваги: підвищені завадостійкійкысть при вузькосмугових і широкосмугових перешкодах, конфіденційність передачі інформації, а також поліпшену електромагнітну сумісність з сусідніми радіоелектронними пристроями.

Широкосмуговий сигнал формується як правило методом прямого розширення спектру з використанням відомих класичних псевдовипадкових послідовностей (ПВП) : m- послідовностей, послідовностей Касами, Голда,,Уолша, які в приймачі можна підібрати і прийняти сигнал.

Мета досліджень. Створення ПВП на основі хаосу, які приймаючий абонент практично не зможе підібрати, і таким чином забезпечити підвищену конфіденційність прийому інформації.

Методика реалізації. З використанням математичної моделі хаотичного логістичного відображення, яка, як показали попередні дослідження, забезпечує найкращі результати, а також звертаючись до біфуркаційної діаграми Фейгенбаума, визначаються параметри 3-х секретних ключів і створюються ПВП вибраної довжини. На основі застосування розробленого в системі МАТЛАБ графічного інтерфейсу користувача здійснюється кореляційний аналіз отриманих ПВП і визначаються ПВП з мінімальним рівнем бічних пелюсток автокореляційної функції.

Результати досліджень. Шляхом емпіричного вибору 3 - х секретних ключів-динамического параметра діаграми Фейгенбаума, початкового значення послідовності і номера початкового імпульсу ПВП, а також дослідження автокореляційної функції отримані ПВП з прийнятним для практичного використання рівнем бічних пелюсток автокореляційної функції не більше 0,25.

Висновки. Використання відомих псевдовипадкових последовательностей-Уолша, Касами, Голда при створенні систем з шумоподібним сигналом не забезпечує повну конфіденційність передачі інформації, оскільки їх можна підібрати в приймачі.

Найбільш прийнятним за критерієм мінімуму бічної пелюстки автокореляційної функції -не гірше 0,25,є використання хаосу на основі логістичного відображення Фейгенбаума.

При створенні псевдовипадкових послідовностей на основі хаосу найкращі результати дає вибір максимального значення динамічного параметра діаграми Фейгенбаума на рівні граничного значення, рівного 4, з точністю 0,05.

Ключові слова: телекомунікаційна система, широкосмуговий псевдошумовий сигнал, логістичне відображення, база сигналу; радіоканал.

Семенко А.И., Кушнир М.Я., Бокла Н.И., Шестопал Ю.О.

Применение псевдослучайной последвательности на основе хаоса для создания широкополосных телекоммуникационных системы с улучшенными характеристиками

Проблематика. Телекоммуникационные системы с широкополосным сигналом имеют несомненные преимущества: повышенные помехоустойчивости при узкополосных и широкополосных помехах, конфиденциальность передачи информации, а также улучшенную электромагнитную совместимость с соседними радиоэлектронными устройствами.

Широкополосный сигнал формируется как правило методом прямого расширения спектра с использованием известных классических псевдослучайные последовательностей (ПСП): m-последовательностей, последовательностей Касами, Голда,,Уолша ,которые в приемнике можно подобрать и принять сигнал.

Цель исследований. Создание ПСП на основе хаоса, которые принимающий абонент практически не сможет подобрать, и таким образом обеспечить повышенную конфиденциальность приема информации.

Методика реализации. С использованием математической модели хаотического логистического отображения, которая, как показали предварительные исследования, обеспечивает наилучшие результаты, а также обращаясь к бифуркационной диаграмме Фейгенбаума определяются параметры 3-секретных ключей и создаются ПСП выбранной длины. На основе применения разработанного в системе МАТЛАБ графического интерфейса пользователя осуществляется корреляционный анализ полученных ПСП и определяются ПСП с минимальным уровнем боковых лепестков автокорреляционной функции.

Результаты исследований. Путем эмпирического выбора 3- х секретных ключей-динамического параметра диаграммы Фейгенбаума, начального значения последовательности и номера начального импульса ПСП, а также исследования автокорреляционной функции получены ПСП с приемлемым для практического использования уровнем боковых лепестков автокорреляционной функции не более 0,25.

Выводы. Использование известных псевдослучайных последовательностей-Уолша, Касами, Голда при создании систем с шумоподобным сигналом не обеспечивают полную конфиденциальность передачи информации, поскольку их можно подобрать в приемнике.

Наиболее приемлемым по критерию минимума бокового лепестка автокорреляционной функции –не хуже 0,25 является использование хаоса на основе логистического отображения Фейгенбаума.

При создании псевдослучайных последовательностей на основе хаоса наилучшие результаты дает выбор максимального значения динамического параметра диаграммы Фейгенбаума на уровне граничного значения, равного 4, с точностью 0,05.

Ключевые слова: телекоммуникационная система, широкополосный псевдошумовой сигнал, логистическое отображение, база сигнала; радиоканал.