UDC 621.396.49

CREATION OF PSEUDO-RANDOM SEQUENCES BASED ON CHAOS FOR FORMING OF WIDEBAND SIGNAL

Anatolii Semenko[1], Nikolai Kushnir[2], Nataliya Bokla[1], Grigoriy Kosovan[2]

[1]State University of Telecommunications, Kyiv, Ukraine, [2]Yuriy Fedkovych Chernivtsi National University Chernivtsi Ukraine

Background. Telecommunication systems with a broadband signal have improved noise immunity, the ability to receive a signal in multipath, as well as electromagnetic compatibility with neighboring radio electronic devices. The use of known pseudo-random sequences to create systems doesn't ensure their high confidentiality due to the possibility of their selection when receiving a signal. A significant increase in the confidentiality of the system can be achieved by using pseudo-random sequences based on chaos.

Objective. The aim of the paper is the development of a technique for creating pseudo-random sequences based on chaos, as well as the analysis of the correlation characteristics of pseudo-random sequences formed on the basis of a chaotic signal.

Methods. Chaotic signals are inherently pseudo-random, but they are generated by deterministic systems. All computer models of chaos are approximations of mathematical chaos. Any analysis of these sequences doesn't allow them to be reproduced and they can't be intercepted, so they have significant advantages when used for spreading the signal spectrum and creating a pseudo noise broadband signal. Sequence selection with an acceptable level of side lobes of the autocorrelation function is carried out by using the developed graphical interface method.

Results. It is shown that, based on the chaos of pseudo-random sequences, it is possible to select sequences with side lobe level up to 0.3, suitable for practical use after analysis of their autocorrelation functions.

Conclusions. Using created chaos based pseudo-random sequences is effective for building broadband single-channel telecommunication systems that have a high degree of confidentiality in the information transmission.

Keywords: broadband signal; chaos; pseudorandom sequence; autocorrelation function; confidentiality of information transmission.

Among various types of existing telecommunication systems, special place belongs to the systems with wideband signals. Their undoubtedly advantage is the increased noise immunity against both narrow- and wideband radio interference and confidentiality of the transmitted information. Telecommunication systems (TCS) with a wideband signal have improved capabilities of signal reception under the influence of multipath propagation and electromagnetic compatibility with neighbouring electronic transmitting devices [1, 2].

The main characteristic of the broadband signal is Signal Base B

$$B = TW, \tag{1}$$

where T – signal's duration; W – width of the signal's spectrum.

For the broadband signal $B \gg 1$.

In the real-life TCS is being influenced by the external interference sources that complicates the good quality signal's reception and internal thermal Gaussian noise of electronic components (hereinafter – noise)

In the case if a third-party narrowband transmitter works close to broadband TCS and there's no intentions to jam the wanted wideband signal, there's a case of the impact of narrowband interfere with width W3 << W.

The ratio of the useful signal to total noise power and interference power on the output of the matched filter is [1]

$$\gamma = 2E/(N_0 + P_з/W) \tag{2}$$

where E – energy of one bit; N_0 – spectral density of thermal noise; $P_з$ – power of the interference.

Obviously, regardless of the specific signal interference band W3, the signal/(noise + interference) ratio at the output of a matched filter behaves as if the noise power were evenly distributed in the signal band W, adding noise with the spectral density $P_з/W$. Moreover, the summary noise has Gaussian noise properties [2].

To neutralize the impact of interference notch filter might be used, which can "cut" the interference from the signal's spectrum. This will also cut part of signal's harmonics and the signal, which occupies part of the free from interference spectrum and has power E_1

$$E_1=E(1-W_з/W), \qquad (3)$$

Then on the output of the matched filter we should get the following signal/(noise + interference) ratio:

$$\gamma_1=\gamma_2(1-W_з/W) \qquad (4)$$

where γ_2 – the actual signal-to-noise ratio on the output of the matched filter with no interference.

Obviously, that the larger signal's bandwidth is in comparison to the spectrum width of the interference signal, the lesser will be the spectral density of additive noise from interference signal to the overall noise spectral density, and the impact of narrowband system on the wanted wideband signal and our TCS performance will be also reduce.

Achieving high noise immunity of TCS with the presence of narrowband obstacle is possible only through the widest possible spread spectrum signal without changing its duration (not taking into account “brute force method” – the increase of transmitter's power).

As a deliberate counteraction to the wideband systems work the wideband signal noise barriers can be used, with interference signal spectrum width exceeding the width of the wanted signal. In this case, the signal / (noise + interference) ratio will also be determined by the formula (2). In order to impact on the TCS performance even more the one should provide a significant excess in noise spectral density of the interference signal over the wanted signal's spectral density of the noise, and the below signal/ (noise power + interference signal power) ratio

$$\gamma=2PB/P_з, \qquad (5)$$

where P – signal power; $P_з$ – interference signal power.

Obviously, that taking into account the power peak limit of the wanted signal and interference the only option to enhance the system's immunity against blocking interference signal is to use ultra-wideband signal with the base B >> 1. It provides 2 times signal processing gain (in B times when using the noise spectral density N_0 instead of $N_0/2$).

In the case there's a need to jam wideband signal effective noise barrier can be organized only after detecting a radio signal which is being transmitted and determine its frequency and spectrum width. The system with a broadband signal must work secretly with the minimum signal's spectral density using special modulation techniques which aren't disclosed to the interference barrier owner. The barrier owner should perform the supersensitive power reception of the signal in the radiometer mode in a wide frequency band.

For the interference barrier owner, it is important to use filter with maximum band pass $W_f \geq W$. Then the restoration of signal/noise ratio at the radiometer's output will be:

$$\gamma_p= \gamma_1/2B. \qquad (6)$$

Obviously, that with increase of signal base it becomes more complicate for the interference owner to detect it. Expansion of the signal with constant energy and duration reduces its signal spectral density, masking it under noise.

Broadband signal is formed by using a number of well-known modulation sequences. Interceptor of the signal can analyze the structure of the signal by just a simple enumeration using a bank of parallel matched filters or filters which can be reassembles consistently, when signal is being received for a long period of time. Another important factor for the system with a broadband signal is its encryption by using encryption keys. In all cases, big value of signal base increases the telecommunication system encryption qualities.

The typical feature of the systems' electromagnetic compatibility is their conflict-free coexistence in one region. In order to achieve this transmitter must emit a minimum signal level in the frequency band of receivers so that the signal spectral density would be less than some threshold value, for example -7dB above the level of noise. The broadband signal enables such functionality, being the one of the most effective ways to ensure electromagnetic compatibility between radio systems.

Wideband signal provides high resolution while receiving pulses with short duration Δt

$$\Delta t=1/W. \qquad (7)$$

In the case if the multipath propagation effect existence of the signal is present, this feature of the wideband systems make possible to identify short duration pulses, which comes to the receiver with some delay due to signal reflection from obstacles. These pulses are being processed by Rake receiver or equalizer, and a total signal is obtained. Such design increases the signal-to-noise ratio at the receiver's output.

In a number of cases, it is appropriate to create a single-channel TCS with a broadband pseudonoise signal, with advantages listed above, which effect can be already seen when the signal base is B = 10-20 dB [2].

The system with modulation performed by a pseudo-random sequence formed from a chaotic signal-chaos will have almost absolute confidentiality.

Chaotic signals are pseudo-random by their nature, but they are generated by systems [3-5]. Any analysis of these sequences does not make it possible to reproduce them and they can't be used for interception of transmitted signal. That's why they have unique advantages when used being for signal spectrum spreading and creating a pseudo noise wideband signal.

It should be emphasized that the chaotic structure of the signal can't be realized on a computer with a finite number of states. Each subsequent state of the system must not coincide with any previous state of the trajectory. Otherwise (for example, as a result of rounding), trajectory of the chaotic signal becomes a cyclic orbit. All computer models of chaos are approximations of mathematical chaos. The approximation passes the properties of the initial system on its initial iterations, but on the boundary of the iteration step n → ∞, the approximation is not accurate enough (that is, the trajectory of the model diverges from the trajectory of the original system). Computer approximations of chaotic mappings are called pseudo-chaos. The behavior of a pseudo-chaotic system can qualitatively differ from the initial chaotic system. At the same time, a pseudo-pseudo-chaotic system can be considered almost unpredictable and irreproducible.

The modified mathematical form of the logistic mapping of a chaotic signal is defined as [4]

$$X_{n+1} = f(X_n) = \lambda X_n (1 - X_n), \qquad (8)$$

where X_n – variable of the state, which is located on 0 – 1 interval; n – iteration number; n = 0, 1, 2, 3,…, ∞; λ – a system parameter, which can have any value in the range from 1 to 4.

Pseudo-chaotic sequences will be implemented with parameters $\lambda > 3.6$ and with iterations number $n > 50$, when the so-called developed chaos is realized. The space of key in this case is the regions of the parameters λ, the initial values of x0 and the iteration number n. Generator of the pseudorandom sequences is based on logistic mapping, which is a one-dimensional chaotic system with one management parameter and one initial condition according to the equation (1).

At the same time x_n is the value of a variable system on step n, λ - control parameter of the logistic mapping that varies in (3.65 ÷ 4) range. The process of doubling the period of chaotic oscillations is shown in Fig. 1.

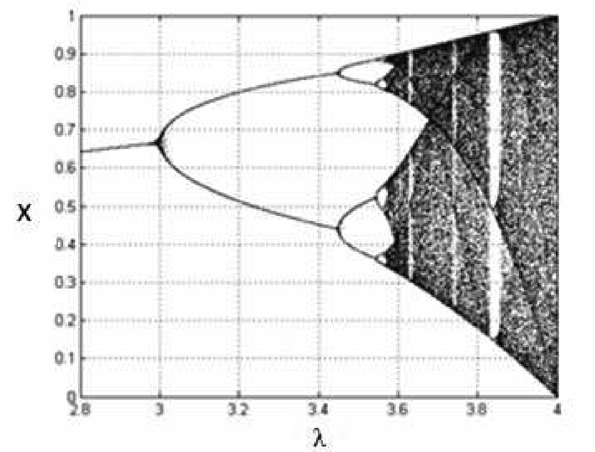


Fig. 1. Bifurcation diagram of the logistic mapping

Generator of the pseudorandom sequences works as follows:

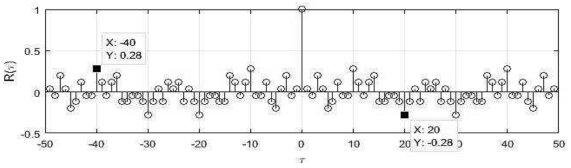
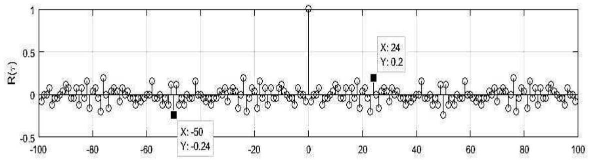
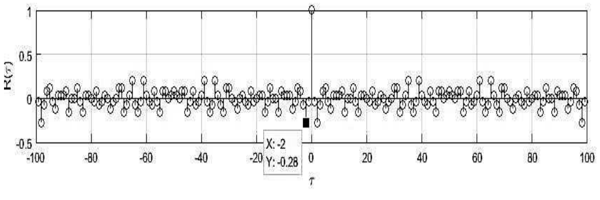
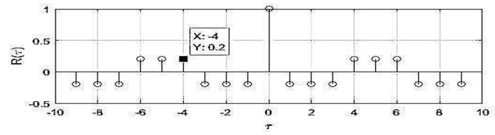
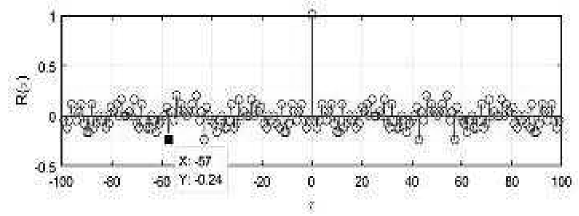
1. Logistics mapping generates the value of variable x during next n given iterations.

2. After each iteration the obtained value is being compared with the given threshold (for example, 0,5) and determine which bit was generated. If the obtained value of the variable x<0,5 then the logical «0» is generated, in other case – logical «1».

During the investigation of this generator functioning it was found that the best properties have the pseudorandom sequence which were generated when the control parameter values λ ∈ (3,95 ÷ 4,0). It was found that it's necessary to select threshold value in order to get the best conditions for balance between the number of bits with logic levels "0" and "1". Using the developed graphical user interface [5], autocorrelation functions (ACFs) of the number of pseudo-random sequences, formed on the basis of dynamic chaos signals, were obtained. Table 1 shows the selected results, for which the ACF has side lobes, which are acceptable for use and which levels don't exceed 0,3 value.

Table 1 uses the notation: N is the number of the variable xn+1 (that is, the values of n + 1) from which the pseudo-random sequence begins, n * is the number of pulses of the pseudo-random sequences short-listed for the ACF study.

Table 1. Auto-correlation functions obtain from the short-listed pseudo-random sequences, obtained from the chaotic signals

<table>
<tr><th>№</th><th>Param. of chaos</th><th>PRS structure</th><th>Max. side lobes</th></tr>
<tr><td>1</td><td>λ=3,99;
x_0=0,35;
N=10;
n*=50</td><td>-1 1 1 -1 1 -1 -1 -1 1 -1 -1 1 -1 -1 -1 1 1 -1 1 1 1 -1 1 -1 -1 1 1 1 1 1 1 -1 1 1 -1 1 -1 -1 1 1 1 1 1 1 1 -1 -1 -1 1 -1</td><td>0,28</td></tr>
<tr><td colspan="4">ACF structure

 </td></tr>
<tr><td>2</td><td>λ=3,99;
x_0=0,35;
N=100;
n*=100</td><td>-1 1 1 -1 1 -1 -1 -1 1 -1 -1 1 -1 -1 -1 1 1 -1 1 1 1 -1 1 -1 -1 1 1 1 1 1 1 -1 1 1 -1 1 -1 -1 1 1 1 1 1 1 1 -1 -1 -1 1 -1 1 1 -1 1 -1 -1 -1 1 1 -1 -1 1 1 -1 1 -1 1 1 -1 -1 -1 1 1 -1 1 1 1 -1 -1 -1 1 -1 1 -1 -1 -1 1 -1 1 -1 -1 1 1 -1 -1 -1 1 -1 -1 -1 1 -1 1 1 1</td><td>0,24</td></tr>
<tr><td colspan="4">ACF structure

 </td></tr>
<tr><td>3</td><td>λ =3,99;
x_0=0,35;
N=500;
n*=100</td><td>-1 1 1 -1 1 1 1 1 1 1 -1 -1 1 -1 1 -1 1 1 -1 -1 -1 1 1 -1 -1 1 -1 1 -1 -1 -1 1 1 -1 -1 1 1 1 -1 -1 1 -1 -1 1 -1 -1 1 1 1 -1 -1 1 -1 -1 1 1 1 1 -1 -1 -1 1 1 -1 -1 1 -1 -1 1 -1 1 1 -1 -1 1 1 -1 -1 -1 1 -1 -1 -1 1 1 -1 1 -1 -1 -1 1 -1 1 -1 -1 -1 1 1 -1 -1</td><td>0,28</td></tr>
<tr><td colspan="4">ACF structure

 </td></tr>
<tr><td>4</td><td>λ =3,99;
x0=0,35;
N=1000;
n*=10</td><td>-1 -1 -1 1 -1 1 -1 -1 1 1</td><td>0,2</td></tr>
<tr><td colspan="4">ACF structure

 </td></tr>
<tr><td>5</td><td>λ =3,99;
x_0=0,35;
N=1000;
n*=100</td><td>-1 -1 -1 1 -1 1 -1 -1 1 1 1 1 1 -1 -1 1 1 1 -1 1 -1 -1 -1 1 -1 1 -1 1 1 -1 -1 -1 1 1 -1 -1 1 -1 -1 1 1 1 -1 -1 1 1 -1 -1 1 -1 -1 -1 1 1 -1 -1 -1 1 1 -1 1 -1 1 1 1 1 1 1 1 1 -1 -1 1 -1 1 -1 -1 1 1 -1 1 1 -1 -1 1 -1 1 1 1 1 -1 1 -1 -1 1 1 -1 -1 -1 1 -1</td><td>0,24</td></tr>
<tr><td colspan="4">ACF structure

 </td></tr>
</table>

While performing the researches it has been found that acceptable ACFs are obtained by the number of impulses in the PRS more than 50, formed by the “cut " from the short sequences, and smaller lengths of the PRSs formed by the "cut" from the long sequences.

The analysis of the cross-correlation functions of these PRSs shows that they have significant levels of lobes that are not acceptable for the practical use of signals, in particular for creating TCS with channels code division.

The results of the correlation PRS functions analysis, which had been obtained from the chaotic signals, were calculated for the first time, and in the known literature sources no similar researches were found.

Conclusion

1. Based on the chaotic signals the pseudo-random sequences of any length can be formed.
2. From the generated pseudo-random sequences on the basis of chaotic signals, with the help of the created graphical user interface, PRS with acceptable auto-correlation function of the side lobes level – no more than 0,3, can be selected.
3. The cross-correlation functions of the PRS, obtained from a chaotic signal, have significant levels of lobes that aren’t acceptable for the practical use of signals.
4. Pseudo-random sequences obtained from the chaotic signal are effective for construction of single-channel TCS with a wideband pseudo-noise signal and absolute confidentiality of the information transmitted by it.

References

1. Ipatov V.P. Broadband systems and code channels division of the signals.- M.:Technospera.2007.-488 p.
2. Sklar B. Digital communications. Fundamentals and Applications. -Translation from English. – M.: Publishing House Ltd «Williams», 2004. – 1104 p.
3. 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.
4. Andrecut M. Logistic map as a random number generator //International Journal of Modern Physics B. - 1998.- Vol. 12.-P. 921-930.
5. Information technologies based on chaos for transmission, processing, storing and protection of the information / U.V. Gulyaev, P.B. Belyaev, G.M. Voroncov and others//Radio technics and electronics. – 2003. – T. 48. – № 10. – p. 1157–1185.
6. Bokla N.I. Research of the PRS correlation properties based on gold code using Mathlab by //Vistnuk DUIKT.- 2011.-Vol.9. - №4.-P.386-391.

Семенко А.І., Кушнір Н.Я., Бокла Н.І., Косован Г. В.

Створення псевдовипадкових послідовностей на основі хаосу для формування широкосмугового сигналу

Проблематика. Телекомунікаційні системи (ТКС) з широкосмуговим сигналом мають покращені завадостійкість, можливість приймання сигналу при багатопроменевому розповсюдженні, а також електромагнітну сумісність із сусідніми радіоелектронними пристроями. Використання відомих псевдовипадкових послідовностей для створення систем не забезпечує їх високу конфіденційність через можливість їх підбору при прийманні сигналу. Суттєве підвищення конфіденційності системи може бути досягнено шляхом використання псевдовипадкових послідовностей на основі хаоса.

Мета досліджень. Розробка методики створення псевдовипадкових послідовностей на основі хаосу. Аналіз кореляційних характеристик псевдовипадкових послідовностей, сформованих на основі хаотичного сигналу.

Методика реалізації. Хаотичні сигнали за своєю природою є псевдовипадковими, але вони генеруються детермінованими системами. Всі комп'ютерні моделі хаосу є апроксимацією (наближення) математичного хаосу. Будь-який аналіз цих послідовностей не дає можливості їх відтворити і вони не можуть бути перехоплених, тому вони мають суттєві переваги при використанні для розширення спектра сигналу і створення псевдошумового широкосмугового сигналу. Відбір послідовностей з прийнятним рівнем бічних пелюсток автокореляційної функції здійснюється шляхом використання розробленого методу графічного інтерфейсу.

Результати досліджень. Показано, що із створених на основі хаосу псевдовипадкових послідовностей можливо відібрати після аналізу їх автокореляційних функцій послідовності з рівнем бічних пелюсток до 0,3, які придатні для практичного використання.

Висновки. Використання створених псевдовипадкових послідовностей на основі хаосу ефективно для побудови широкосмугових одноканальних телекомунікаційних систем, що володіють підвищеною конфіденційністю передачі інформації.

Ключові слова: широкосмуговий сигнал; хаос; псевдовипадкова послідовність; автокореляційна функція; конфіденційність передачі інформації.

Семенко А.И., Кушнір Н.Я., Бокла Н.И., Косован Г. В.

Создание псевдослучайных последовательностей на основе хаоса для формирования широкополосных сигналов

Проблематика. Телекоммуникационные системы (ТКС) с широкополосным сигналом имеют улучшенные помехоустойчивость, возможность приема сигнала при многолучевом распространении, а также электромагнитную совместимость с соседними радиоэлектронными устройствами. Использование известных псевдослучайных последовательностей для создания систем не обеспечивает их высокую конфиденциальность из-за возможности их подбора при приеме сигнала. Существенное повышение конфиденциальности системы может быть достигнуто путем использования псевдослучайных последовательностей на основе хаоса.

Цель исследований. Разработка методики создания псевдослучайных последовательностей на основе хаоса. Анализ корреляционных характеристик псевдослучайных последовательностей, сформированных на основе хаотического сигнала.

Методика реализации. Хаотические сигналы по своей природе псевдослучайными, но они генерируются детерминированными системами. Все компьютерные модели хаоса является аппроксимацией (Приближение) математического хаоса. Любой анализ этих последовательностей не дает возможности их воспроизвести и они не могут быть перехваченных, поэтому они имеют существенные преимущества при использовании для расширения спектра сигнала и создания псевдошумового широкополосного сигнала. Отбор последовательностей с приемлемым уровнем боковых лепестков автокорреляционной функции осуществляется путем использования разработанного метода графического интерфейса.

Результаты исследований. Показано, что из созданных на основе хаоса псевдослучайных последовательностей возможно отобрать после анализа их автокорреляционной функций последовательности с уровнем боковых лепестков до 0,3, пригодные для практического использования.

Выводы. Использование созданных псевдослучайных последовательностей на основе хаоса эффективно для построения широкополосных одноканальных телекоммуникационных систем, обладающих повышенной конфиденциальности передачи информации.

Ключевые слова: широкополосный сигнал; хаос; псевдослучайная последовательность; автокорреляционная функция; конфиденциальность передачи информации.