THE COMPARISON OF DISCRETE TIME MAPS AS CHAOTIC CARRIER SOURCE FOR INFORMATION TRANSMISSION SYSTEM

M.V. Larionova, A.S. Petrov
e-mail: fks@srv-vmss.mpei.ac.ru

Moscow Power Engineering Institute (Technical University)
14, Krasnokazarmennaya st. Moscow E-250, 111250, Russia

Abstract *– From the point of view of the requirements presented by communication systems to the chaos generator, in this paper a class of ramp periodic functions as a map generating chaotic oscillation are introduced. The must important properties of this map in comparison with well-known logistic map are studied, also the analysis of these maps concerning to inverse problem of nonlinear dynamics known from a number of papers are carried out.*

1. INTRODUCTION

Recently the application of chaos in the communication system (CS) became a very actual problem thanks to a number of chaotic waveforms useful properties – Ref. 1. For the estimation of the transmitted information immunity extent from unauthorized access the chaotic dynamics inverse problem must be solved, that is we must to restore transmitted information from the mixture of chaotic signal and noise. When a priori information is absent its solution difficulty are tremendous. In this case for the problem put by successful solution a part of information about transmitted side the authors assume known, namely the type of dynamical system (DS) generating a chaotic waveforms, the modulation method and structure of the receiver. The choice of DS, generating chaotic oscillation, and modulation method are the direct problem of chaotic dynamics. As a source of chaotic waveforms nonlinear continuous-time systems and a wide class of nonlinear discontinuous functions (maps) are used. Among chaos generators with discontinuous time the one-parameter maps are the most extensively used at present, namely the logistic map, "tent-map" and shift map. These maps are used as chaos generators in most works studying CS based on chaos. But in literature the question: "How much are these maps suitable for CS?" – hasn't solved completely yet.

In this paper we propose a ramp map as a chaotic generator in CS with chaotic carrier and consider its properties conformably to inverse problem decision.

2. PROBLEM STATEMENT

At choice of the type of a map used as a source of controllable chaotic sequences in the CS with chaotic carrier, it is necessary to take into account a number of requirements:

- Nonlinear functions of maps mustn't be one-to-one simple.
- The chaotic regime must be stable and must arise independently of initial conditions.
- The change range of a map controlling parameter corresponding to the chaotic regime should be maximum length. Inside this interval the regularity windows must be absent.
- The change of the map controlling parameter should not lead to considerable changes of such characteristics as the chaotic sequences average of distribution and dispersion.

From the point of view of the requirements mentioned above the authors introduces a class of ramp periodic functions as a chaotic waveforms generator:

$$F(a,x)=2ax-2n \qquad x\in\left[\frac{n}{a}-\frac{1}{2a};\frac{n}{a}+\frac{1}{2a}\right],$$

$$a>1,\ n=..-2,-1,0,1,2... \qquad (1)$$

This map is the private case of the Bernoulli shift map and it is depicted in fig.1 (a=1.9, x_0=0.3). The Lamerey-Kennings diagram and time realization are shown in the fig. 2, 3 accordingly. The ramp map was considered in comparison with well known from literature logistic map:

$$F(\lambda,x)=\lambda x(1-x) \qquad (2)$$

where λ = 3.9 – is the parameter of map, the initial condition (IC) $x(0)$ belongs to the interval (0,1). In fig. 4 and 5 bifurcation diagrams for logistic and ramp maps are depicted. One can see that the logistic map controlling parameter has limited range of change with wide window of regularity inside this range. The ramp map hasn't this deficiency, besides the change of the ramp map controlling parameter doesn't lead to considerable changes of the chaotic sequences mean value and dispersion.

Now let us consider a CS with chaotic carrier using these maps. As a method of the modulation at the transmitter we use the digital binary modulation method, well known from literature – Ref. 2 as a Chaos Shift Keying (CSK), namely the initial conditions manipulation method. In case of the authorized access to the information the optimal correlative receiver demonstrated in fig. 6 is used. It is known – Ref. 3, that this receiver is guaranteed the best noise immunity in case of the use of regular signals. At unauthorized access solving blocks collection are added to the correlation receiver. The structure of these blocks is determined by a priory information completeness about transmitted system. In this case we can divide the inverse problem in next subproblem:

1. The synchronization recover
2. The determination of the map dimension
3. The map type restoration
4. The map parameter and initial conditions reconstruction

Further in this paper we will consider the problem of the IC reconstruction proposing that synchronization has been recovered, as a chaos generator ramp and logistic maps are used, and its parameter are known. But at first let us view the authorized receiver characteristics, namely the bit error ratio (BER) dependence from signal-to-noise ratio (SNR) and the parameter and IC error value influence on the BER.

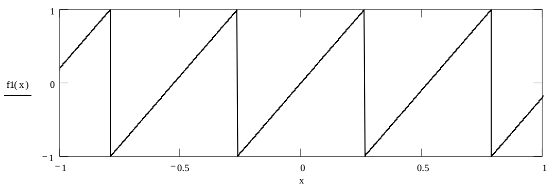

Fig. 1 Ramp function

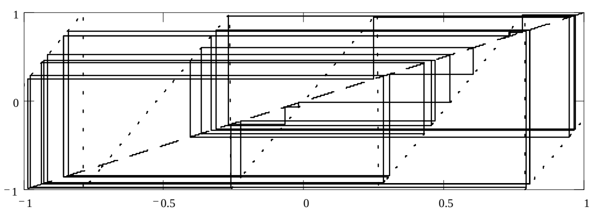

Fig. 2 Lamerey-Kennings diagram

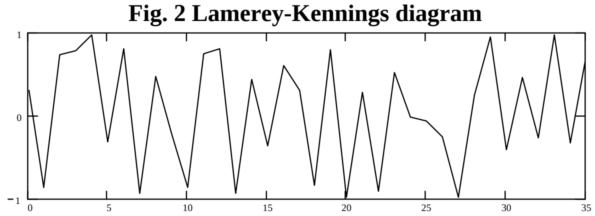

Fig. 3 Time realization

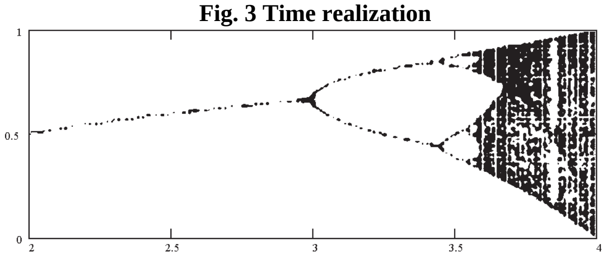

Fig. 4 Bifurcation diagram of the logistic map

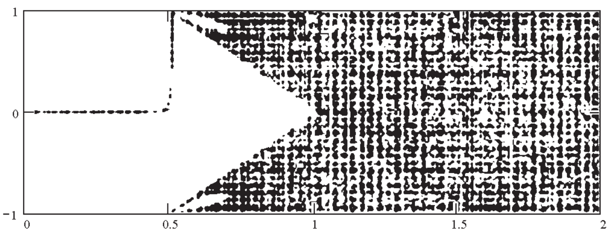

Fig. 5 Bifurcation diagram of the ramp map

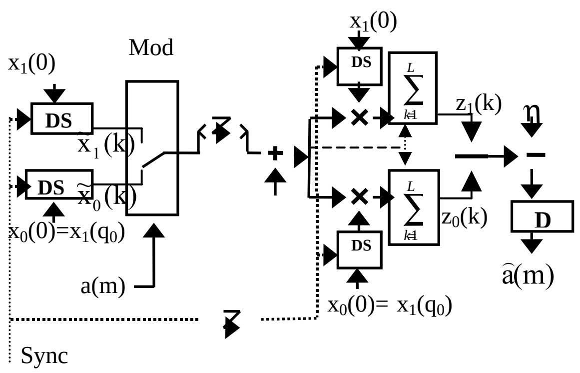

Fig. 6 The structure of the chaotic signal correlation receiver

3. PROBLEM DECISION

For the correlation receiver of regular signals it is known from literature the next expression for the BER:

$$P_{err} = 1 - \Phi\left[\sqrt{\frac{E*(1-r_s)}{2*\sigma^2}}\right] \tag{3}$$

where $\Phi(z) = \frac{1}{2\pi}\int_{-\infty}^{z}\exp\left(\frac{-t^2}{2}\right)dt$ -the gaussian probability integral, $E = \sum_{k=1}^{L}\tilde{x}_0^2(k) = \sum_{k=1}^{L}\tilde{x}_1^2(k)$ - the energy of elementary signals $\tilde{X}_0(k)$ and $\tilde{X}_1(k)$, σ^2 – the noise n(k) dispersion, $r_s = \frac{1}{E}\sum_{k=1}^{L}\tilde{x}_1(k)\,\tilde{x}_0(k)$ – the correlation coefficient of elementary signals $\tilde{X}_0(k)$ and $\tilde{X}_1(k)$.

It is evident (see (3)) that for the BER decrease the initial conditions $\tilde{X}_0(0)$ and $\tilde{X}_1(0)$ must correspond to zeros or negative values of the correlation coefficient r_s. We suppose that different initial conditions $\tilde{X}_0(0)$ and $\tilde{X}_1(0)$ correspond to chaotic sequence $\tilde{X}(k)$ shifted on the whole number of time intervals k. The fig. 7 shows the autocorrelation function of chaotic sequence $\tilde{X}(k)$ defined by the formula:

$$r_s(q) = \frac{1}{E}\sum_{k=1}^{K}\tilde{x}_1(k)\tilde{x}_1(k+q) \tag{4}$$

for the logistic map (curve 1) and ramp map (curve 2). The zero and negative values of the autocorrelation function correspond to the shifts in 1, 2 etc. intervals of a discrete time.

It is known that chaotic sequences are very sensitive for an accuracy of initial conditions and parameter establish. In real systems initial conditions and parameter are established with limited accuracy, therefore BER increases in comparison with formula (3). In fig. 8 the dependencies of BER from SNR are shown for the logistic map. The theoretical curve (curve 1) is calculated by the formula (3), the experimental curves are obtained by computer simulation of the CS for the cases of precise establish of initial conditions and parameter and for non-precise one. As it is mentioned above the parameters establish errors of the bearing signals result in information restoration worsening. Physically the error of the parameter or initial conditions establishes means the change of the autocorrelation function kind. At this conditions the q value shifts, before corresponded to zero or negative correlation coefficient values, can result in positive correlation coefficient values. This phenomenon in accordance with the formula (3) increases BER.

In fig. 9 the dependence of the BER from SNR is shown for logistic map in comparison with this dependence for the ramp map. On this curves experimental points are plotted. As one can see f+rom this diagram the BER for ramp map is greater than for logistic map, since the logistic map correlation coefficient (r_s = -0.575) at used parameters (λ = 3.9, x_0 = 0.1) in absolute value are greater than that (r_s = -0.402) for ramp map. Thereupon the choice of optimal parameters proportion of ramp map for maximum (in absolute value) correlation coefficient obtaining is interesting problem.

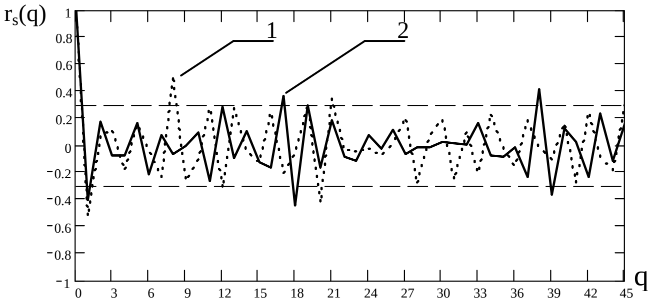

Fig. 7 Autocorrelation function for the logistic (curve 1) and ramp (curve 2) maps

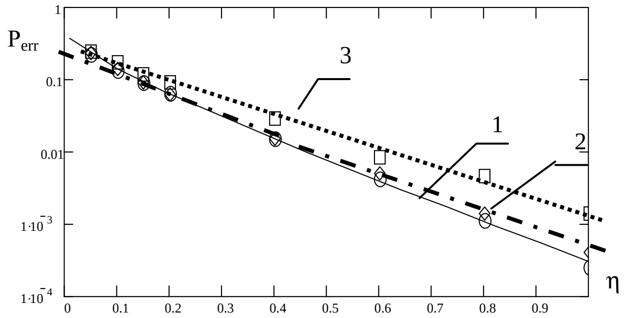

Fig. 8 The dependence of the BER from SNR for parameter establish error (curve 1: x_0=0.1, λ=3.9; curve 2: P_0=0.1, λ=3.9001; curve 3: P_0=0.1001, λ=3.9)

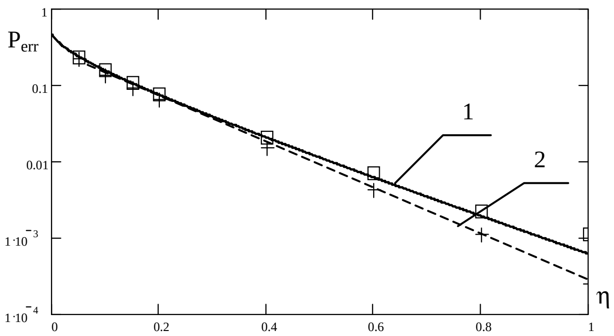

Fig. 9 The dependence of the BER from the SNR
Curve 1 - for the ramp map (Φ= 1.9, s_0 = 0.3)
Curve2 - for the logistic map (λ = 3.9 s_0 = 0.1)

All mentioned above are relative to the authorized access receiver, when all parameters of the transmitted signal are a priori known. The unauthorized access receiver doesn't have a priory information about a structure, parameters and a synchronization method of the dynamical system used at the transmitter. Nevertheless in some special case a problem of the unauthorized access can be decided. Algorithms permissive to get the bearing signals in case, when only initial conditions of the chaotic signals $\tilde{x}_o(k)$ and $\tilde{x}_1(k)$ forming are unknown, are described in the literature – Reff. 4 - 8. One of the possible methods of the initial conditions recover is the filtration algorithm with following interpolation algorithm. These algorithms have the following kind:

Filtration algorithm:

$x_f(k+1) = F(x_f(k))+K(k)*(y(k+1)-F(x_f(k)))$,

where

$F(x(k))=\lambda*x_f(k-1)(1-x_f(k-1))$,

$$K(k)=\left[1+\frac{1}{\left(\frac{d}{ds}F(x)\Big|_{x=x_f(k)}\right)^2}\right]^{-1}$$

Interpolation algorithm: $x(k-1) = F(x(k))^{-1}$

After initial conditions determination the bearing signals are formed. The subsequent processing algorithm is similar to authorized access receiver one. In fig. 10 the dependence of the final count absolute error after filtration operation from SNR for logistic map is depicted. One can see that this algorithm efficiency are small, therefore in some private case to decrease a time of calculation it is possible to exclude this operation.

It is evident that it is impossible to exactly install the IC for the unauthorized access receiver. As it is seen from fig. 11, on which the dependence of the IC restoration absolute error from SNR is represented for logistic map, to take the IC reconstruction error not higher than third character after comma and to work with effective accumulation interval the SNR mustn't be higher 5.5. In that case BER equals about 10^{-6}. In the general way the BER for an unauthorized receiver is higher than that for authorized one. This phenomenon is depicted in fig. 12.

In case of above-mentioned reception algorithms use ramp map ensures a better transmitted information security, than logistic map does. It is shown in fig. 13, 14. Since at calculation of the inverse multiple-valued function it is necessary to use two filtered consequence valuations on each step (previous one and current one), even little noise can result in false IC calculation. Therefore (see fig.13) the IC restoration precision for the ramp map is much less than that for the logistic map. The BER in that case at SNR equaled 1.5 (3.5 dB) is 60 times greater than that for logistic map (see fig.14). Thus we come to conclusion that introduced ramp map satisfies produced requirement; it demonstrates noise-immunity of the authorized access receiver not worse than that at the use of the logistic map; at the same time it guaranties better security of the information transmission. To construct unauthorized access receiver using a ramp map we should use another algorithms (for example, following algorithm) of the IC calculation.

4. CONCLUSION

In this paper the authors have been introduced ramp periodical function as a chaos generator in the CS with a chaotic carrier. Some important properties of this map were studied conformably to the private statement decision of the inverse problem of the chaotic dynamics. It was shown that ramp map ensures better transmitted information security than widely used logistic map does.

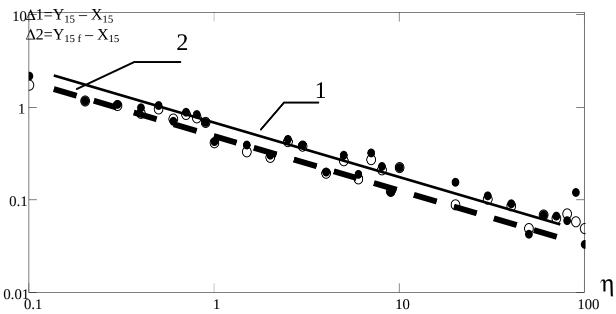

Fig. 10 The dependence of the absolute error from the SNR for the logistic map
curve 1 - the absolute error between the received signal and transmitted signal, curve 2 - the absolute error between the filtered received signal and transmitted signal

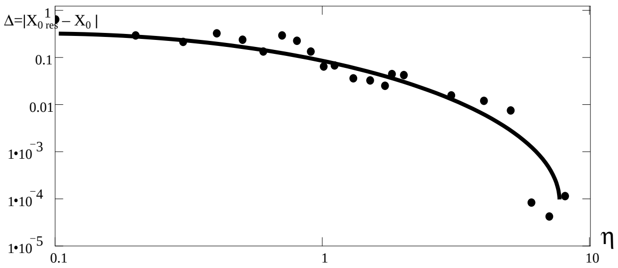

Fig. 11 The dependence of the absolute error between the restored initial condition and starting initial condition from the SNR for the logistic map

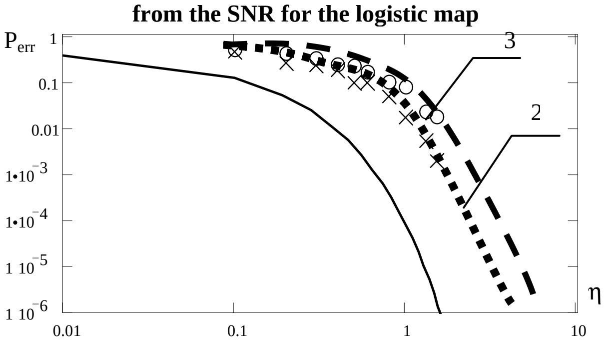

Fig. 12 The dependence of the BER from SNR for unauthorized access receiver for logistic map (curve 2: r_s=0.7, curve 3: r_s=0.775, solid line corresponds to formula (3) r_s=-0.575)

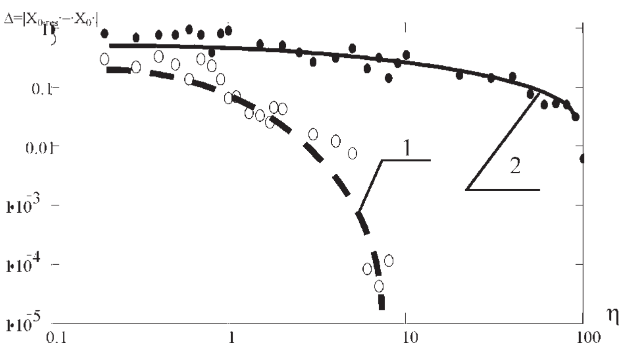

Fig. 13 The dependence of the absolute error between the restored initial condition and starting initial condition from the SNR
curve 1 – for the logistic map, curve 2 – for the ramp map

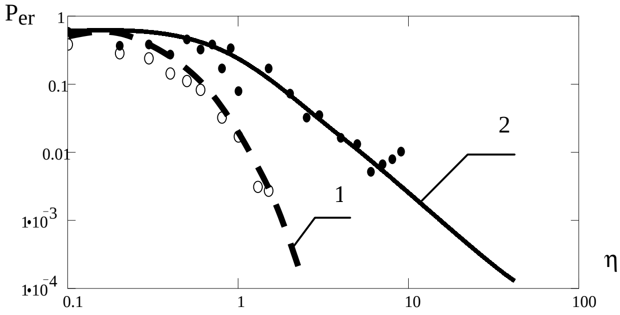

Fig. 14 The dependence of the BER from the SNR for the unauthorized receiver:
Curve 1 – for the logistic map, curve 2 – for the ramp map

REFERENCES

1. Дмитриев А. С., Старков С. О. Передача сообщений с использованием хаоса и классическая теория информации. // *Зарубежная Радиоэлектроника. Успехи современной радиоэлектроники*. № 11, 1998 , с. 4 – 32.
2. Didieu H., Kennedy M. P. and Hasler M. Chaos Shift Keying Modulation and Demodulation of a Chaotic Carrier Using Self-Synchronizing Chua's Circuits. // IEEE Trans. Circ. Syst. , 1993, Part II, vol. 40, pp. 634 – 642.
3. Котельников В. А., Теория потенциальной помехоустойчивости. – М.: Госэнергоиздат, 1956
4. Kuleshov V. N., Larionova M. V., Udalov n. N. Information transmission system using chaotic carrier: demands to the accuracy of symbols generation. // Proceedings International Symposium on Acoustoelectronics, Frequency Control and Signal Generation, St-Petersburg, Russia, 7 - 12 June 1998, pp. 192 - 199.
5. Капранов М.В., Кулешов В.Н., Ларионова М.В., Морозов А.Г., Удалов Н.Н. Свойства систем передачи информации с манипуляцией параметрами и начальными условиями генераторов хаотических колебаний. // «*Зарубежная радиоэлектроника. Успехи современной радиоэлектроники*», № 11, 2000 г., с. 48 – 60.
6. Larionova M. V., Petrov A. S., The Estimate of Symbol Error Probability in the Communication Systems with Chaotic Carrier. // Proceedings of the IV Int. Conference for Young Researchers on Wave Electronics and Its Applications in the Information and Telecommunication Systems, St-Petersburg, Russia, 28 – 31 May, 2001, pp. 36 – 37.
7. Петров А. С. Оценка вероятности приема символа в системах связи с хаотической несущей. // Тезисы докладов 7ой международной научно-технической конференции студентов и аспирантов, 27 – 28 февраля 2001 г., Москва. т. 1. сс. 42 – 43.
8. Петров А. С. Исследование различных дискретных отображений как генераторов хаотической несущей для систем скрытной связи. // Тезисы докладов 8ой международной научно-технической конференции студентов и аспирантов, 28 февраля – 1 марта 2002 г., Москва. т. 1. сс. 39 – 40.