Jurnal Informatika
Vol. 15, No. 1, January 2021, pp. 56-67
ISSN 1978-0524 (print) | 2528-6374 (online)
http://journal.uad.ac.id/index.php/JIFO/index

Transformation of the generalized chaotic system into the discrete-time complex domain

Nina Volianska [a,1,*], Oleksandr Sadovoi [b,2], Roman Voliansky [b,3]

[a] Power Engineering Department, 2, Str. Dniprobudivska, Kamyanske,51918, Ukraine
[b] Electrical Engineering Department, 2, Str. Dniprobudivska, Kamyanske,51918, Ukraine
[1] ninanin@i.ua*; [2] sadovoyav@ukr.net; [3] voliansky@ua.fm
* Corresponding Author

Received 21 Janaury 2021; accepted March 5 2021; March 5 2021

ABSTRACT

The paper deals with the development of the backgrounds for the design and implementation of secured communications by using systems with chaotic dynamics. Such backgrounds allow us to perform the stable transformation of a nonlinear object into a simpler form and formulate the nonlinearities simplification optimization algorithm. This algorithm is based on the optimization problem's solution, which makes it possible to define polynomial order, approximation terms, and breakpoints. Usage of proposed algorithms is one of the ways to simplify known chaotic system models without neglecting their unique properties and features. We prove our approach by considering simplifying the Mackey-Glass system and transforming it into a discrete-time complex domain. This example shows that the transformed system produces chaotic oscillations with twice-increased highest Lyapunov exponent. This fact can be considered as improving the unpredictability of the transformed system and thus it makes background to make highly non-intercepted and undecoded transmission channels.

Check for updates

KEYWORDS
Chaotic dynamic
Secured communications
Complex and hypercomplex numbers
Lyapunov exponent
Tustin transformation

1. Introduction

The problem of data hiding and its secure transmission is known as the cryptography problem [1]. The history of this problem starts in the human civilization dawn and in various times it solves in the different ways. At the beginning of data hiding, they replace symbols from one alphabet to another, then in the medieval polyalphabetic codes are used. At the beginning of the XX century, various electromechanical encryption devices become widely used; the most known is the Enigma machine. These methods use the so-called secret key to encode and decode messages, and both submitter and receiver should know this key to communicate with each other.

Since the end of the nineteen seventies, cryptography gets strong mathematical backgrounds [2]–[4], and now cryptography is considered a symbiosis of math and informatics. Today's symbiosis results are widely used in, such as e-commerce, e-documents exchanging, and telecommunication [5].

One modern cryptography branch uses dynamical chaos to hide transmitted data in unpredictable noise-like signals [6], [7]. A considerable number of research is devoted to studying and designing chaotic oscillators known at the moment [8]–[16]. These researches can be grouped into several groups. The first gives information about mathematical study known chaotic systems and design novel ones [17]–[21]. The second one is devoted to using various transformation techniques to design a new chaotic system from old ones [22]–[26]. The third describes the practical implementation of the designed chaotic systems [27]–[31].

The main feature of the known chaotic system is nonlinear functions in the equations of their motions. Sometimes these functions can be very complex, and it can cause problems with their implementation.

Jurnal Informatika
Vol. 15, No. 1, January 2021, pp. 56-67

That is why the chaotic system's design with simple nonlinearities and increased chaotic features is a significant problem.

We offer to solve this problem by applying piecewise approximation for nonlinear functions. The approximation of the nonlinear functions by piecewise linear ones is a well-known control approach [32], [33]. We suggest extending this approach to some in general case piecewise nonlinear functions simpler than the given nonlinear functions. We use complex numbers to make the system dynamic more unpredictable.

Our paper is organized as follows: at first, we consider a free motion of the generalized nonlinear system and transform it into the discrete-time domain by applying the Tustin transformation. Then we use a polynomial approximation to simplify the system nonlinearities. We consider this approximation from the optimization theory viewpoint. We define approximation polynomial order, its terms, and breakpoints to solve this problem for a minimum of integral between initial and approximated nonlinear function. The solution to this problem makes us formulate an optimized approximation algorithm. At third, we offer to increase system encryption properties by extending phase space where this system is defined we complex and/or hypercomplex numbers. Then we show an example for transforming the Mackey-Glass system into the complex discrete-time domain with cubic splines nonlinear function. At last, we conclude.

2. Method

2.1. Transformation of the Dynamical Object Model into Piecewise Form

Let us consider a generalized nonlinear ordinary matrix differential equation (1)

$$s\mathbf{Y} = \mathbf{F}(\mathbf{Y}), \tag{1}$$

here s=d/dt is a derivative operator, **Y** is a n-th sized state space vector (2)

$$\mathbf{Y} = (y_1\ y_2\ \dots\ y_n)^T \tag{2}$$

where y_i is a i-th state variable,

$$\mathbf{F}(\mathbf{Y}) = (f_1(\mathbf{Y})\ f_2(\mathbf{Y})\ \dots\ f_n(Y)^T \tag{3}$$

where $f_i(\mathbf{Y})$ is some nonlinear function (3).

It is necessary to remark that function fi(**Y**) can be as complicated as defining an object dynamically. One can use elementary functions and algebraic operations for its description, or he can use some non-elementary functions even define it in a non-analytical way. In the last case, it is tough to use well-known analytical approximation approaches based, for example, on the Taylor series [34].

We offer to avoid this drawback by replacing the continuous-time simulation problem (1) with its discrete-time approximation. This approximation can be built by replacing continuous-time derivative with its discrete analogs. The simplest of them are forward and backward differences implemented by using the following well-known expressions [35].

$$s \approx \frac{z-1}{T};\ s \approx \frac{1-z^{-1}}{T} \tag{4}$$

here z is a forward shift operator, and z^{-1} is a backward shift operator, T is a sample time.

It is a well-known fact that approximations (4) do not guarantee the transformed objects' stability, so we suggest using Tustin transformation [36].

$$s \approx \frac{2}{T}\frac{1-z^{-1}}{1+z^{-1}} \tag{5}$$

Approximation (5) makes us the possibility to rewrite (1) as follows

$$\mathbf{Y} - \frac{T}{2}\,\mathbf{F}(\mathbf{Y}) = z^{-1}\mathbf{Y} + \frac{T}{2}\,z^{-1}\mathbf{F}(\mathbf{Y}) \tag{6}$$

Vol. 15, No. 1, January 2021, pp. 56-67 ISSN 2086-8138 (print) | 2745-7249 (online)

If one solves left-hand expression in (6) he finds such an inverse function $\mathbf{F}^{-1}(\mathbf{Y})$ that allows defining its argument in the following way

$$\mathbf{Y} = \mathbf{F}^{-1}\left(\mathbf{Y} - \frac{T}{2}(\mathbf{F}(\mathbf{Y})\right) \tag{7}$$

It is clear that due to equality (6) it is possible to rewrite (7) in such a way

$$\mathbf{Y} = \mathbf{F}^{-1}\left(z^{-1}\mathbf{Y} + \frac{T}{2}\, z^{-1}(\mathbf{F}(\mathbf{Y})\right) \tag{8}$$

If function $\mathbf{F}(\mathbf{Y})$ is the time-independent function, (8) can be written down as follows

$$\mathbf{Y} = \mathbf{F}^{-1}\left(z^{-1}\mathbf{Y} + \frac{T}{2}\, \mathbf{F}(z^{-1}\mathbf{Y}\right) \tag{9}$$

Matrix expression (9) allows us to define current values of state variables by their previous values, and one can find that (9) is similar to some numerical integration schemes.

We will call (9) a discrete-time model for the considered object. This model's main difference from the original one is an operating with values of nonlinear function F(Y) but not its analytical description. Contrary to model (1), model (9) can be easily implemented with any PC mathematical software. This model can be considered the set of points in the fixed time moments, and any symbolical computations or transformations are not required.

Nevertheless, one can find some difficulties in using (9) because of the nonlinear function F(Y). Instead of dramatically increasing the modern PCs' computational resources, it can require a lot of processor time to calculate its values and values of the inverted function in every time moment. Moreover, if F(Y) is given by table of its values and arguments, it is unclear what to do if the calculated argument does not correspond to Table 1. Different machine learning techniques can be used to solve this uncertainty and build the model with AI elements.

We leave these possibilities for future studying and consider here the piecewise approximation of a nonlinear function.

In the simplest case, such approximation gives us the following expression for the nonlinear single variable function (10).

$$\hat{f}_i(y) = \begin{cases} c_{1j}y + c_{0j} & if \quad y_{ij} < y_i < y_{i(j+1)}; \\ c_{1(j+1)}y + c_{0(j+1)} & if \quad y_{i(j+1)} < y_i < y_{i(j+2)}; \\ \vdots & \vdots \qquad \vdots \\ c_{1(j+k)}y + c_{0(j+k)} & if \quad y_{i(j+k-1)} < y_i < y_{i(j+k)}, \end{cases} \tag{10}$$

Here cij are linear approximation terms, yij are breakpoints of the nonlinear function, k is several breakpoints.

It is clear that if the number of breakpoints equals the number of simulation steps, the piecewise function (10) becomes a simulation point table. This function can be considered a linear approximation function in other cases.

If one considers multivariate function, he can replace line equations in (11) with hyperplane equations in some multidimensional space

$$\hat{f}_i(y_1, y_2, \dots, y_n) = \begin{cases} \sum_{u=1}^{n} c_{1ju}y_u + c_{0j} & if \quad y_{uj} < y_u < y_{u(j+1)}; \\ \sum_{u=1}^{n} c_{1(j+1)u}y_u + c_{0(j+1)} & if \quad y_{u(j+1)} < y_u < y_{u(j+2)}; \\ \vdots & \vdots \qquad \vdots \\ \sum_{u=1}^{n} c_{1(j+k)u}y_u + c_{0(j+k)} & if \quad y_{u(j+k-1)} < y_u < y_{u(j+k)}, \end{cases} \tag{11}$$

Jurnal Informatika
Vol. 15, No. 1, January 2021, pp. 56-67

In the most general case, line and plane equations can be replaced with some simpler function than the initial one, i.e., one can use single and multivariate polynomial to define piecewise functions for each interval. In this case, (12) and (13) can be rewritten as follows

$$\hat{f}_i(y)=\begin{cases}\sum_{l=0}^{m} c_{jl} y_i^l & if \quad y_{ij}<y_i<y_{i(j+1)};\\ \sum_{l=0}^{m} c_{(j+1)l} y_i^l & if \quad y_{i(j+1)}<y_i<y_{i(j+2)};\\ \vdots & \vdots \qquad \vdots \\ \sum_{l=0}^{m} c_{(j+k)l} y_i^l & if \quad y_{i(j+k-1)}<y_i<y_{i(j+k)},\end{cases} \tag{12}$$

here m is an order of approximation polynomial, and

$$\hat{f}_i(y_1,y_2,\dots,y_n)=\begin{cases}\sum_{l_1=0}^{m}\cdots\sum_{l_n=0}^{m} c_{jl} y_{l_1}\cdots y_{l_n} & if \quad y_{l_i j}<y_{l_i}<y_{l_i(j+1)};\\ \sum_{l_1=0}^{m}\cdots\sum_{l_n=0}^{m} c_{(j+1)l} y_{l_1}\cdots y_{l_n} & if \quad y_{l_i(j+1)}<y_{l_i}<y_{l_i(j+2)};\\ \vdots & \vdots \qquad \vdots \\ \sum_{l_1=0}^{m}\cdots\sum_{l_n=0}^{m} c_{(j+k)l} y_{l_1}\cdots y_{l_n} & if \quad y_{l_i(j+k-1)}<y_{l_i}<y_{l_i(j+k)}.\end{cases} \tag{13}$$

Thus, piecewise function (12) and (13) allows us to simplify the simulation of generalized nonlinear objects (1) and (8) and reduce calculation time for significant nonlinear object simulation. We use polynomial functions to define initial function approximation in the j-th interval because they allow getting near zero roots measured square deviation.

2.2. Algorithm for Approximation Functions Optimization

The approximation accuracy of equation equations and approximation accuracy is defined by values of the approximation terms c_{ij} and the number of breakpoints k and order m.

We assume that the desired approximation accuracy ε is known, and the maximal order of approximation polynomial m_{max} is defined from the implementation complexity viewpoint.

1. Number of breakpoints is assumed equals to some positive non-big number
2. Polynomial order is assumed to be one
3. Approximation terms are defined as state variables and breakpoints functions (14)

$$c_{ij}=g_{ij}(\mathbf{Y},\mathbf{Y_u}), \tag{14}$$

   here **Yu** is a matrix of breakpoints coordinates
4. Following cost function (15)

$$\mathbf{I}=\int_{\mathbf{Y_{min}}}^{\mathbf{Y_{max}}}\left|\mathbf{F}(\mathbf{Y})-\hat{\mathbf{F}}(\mathbf{Y})\right|dy, \tag{15}$$

   here **Ymin, Ymax** are vectors of maximal and minimal values of state variables,

   is calculated for current values of state variables
5. Coordinates of breakpoints are defined after the solution of the minimization problem for the (16)

$$\mathbf{I} = \int_{\mathbf{Y}_{\min}}^{\mathbf{Y}_{\max}} \left|\mathbf{F}(\mathbf{Y}) - \hat{\mathbf{F}}(\mathbf{Y})\right| dy \to \min_{\mathbf{Y}_u}, \qquad (16)$$

6. If the minimum of the cost function defined for optimized breakpoints is bigger than desired accuracy ε, and order m is less than mmax, we increment m by one and continue the algorithm from the third points.
7. If order m becomes equal to mmax, we increase the number of breakpoints by one. The algorithm is restarted from the second point.
8. Algorithm stops if the desired accuracy achieved or maximal polynomial order with the maximal desired number of breakpoints and obtained. In the first case, optimization is considered as completed. In the second one, it is necessary to increase approximation accuracy or change approximation function.

Due to the high formalization of the proposed algorithm, it is necessary to implement it by different mathematical software and program language. Minimizing the cost function, which means the absolute value of square between initial nonlinear function and approximation, can be performed using standard optimization routines, such as particle swarm optimization [37].

2.2. Research Method

The use of the proposed approach makes us the possibility to transform (1) and rewrite it in the continuous-time domain

$$sy_i = \begin{cases} \sum_{l_1=0}^{m}\cdots\sum_{l_n=0}^{m} c_{jl} y_{l_1}\cdots y_{l_n} & \text{if} \quad y_{l_i j} < y_{l_i} < y_{l_i(j+1)}; \\ \sum_{l_1=0}^{m}\cdots\sum_{l_n=0}^{m} c_{(j+1)l} y_{l_1}\cdots y_{l_n} & \text{if} \quad y_{l_i(j+1)} < y_{l_i} < y_{l_i(j+2)}; \\ \vdots & \vdots \qquad \vdots \\ \sum_{l_1=0}^{m}\cdots\sum_{l_n=0}^{m} c_{(j+k)l} y_{l_1}\cdots y_{l_n} & \text{if} \quad y_{l_i(j+k-1)} < y_{l_i} < y_{l_i(j+k)}. \end{cases} \quad i = 1,\ldots,n, \qquad (17)$$

and in the discrete-time domain

$$y_i = f_i^{-1}\left(z^{-1} y_i + \frac{T}{2} \begin{cases} \sum_{l_1=0}^{m}\cdots\sum_{l_n=0}^{m} c_{jl} z^{-1} y_{l_1}\cdots z^{-1} y_{l_n} & \text{if} \quad y_{l_i j} < y_{l_i} < y_{l_i(j+1)}; \\ \sum_{l_1=0}^{m}\cdots\sum_{l_n=0}^{m} c_{(j+1)l} z^{-1} y_{l_1}\cdots z^{-1} y_{l_n} & \text{if} \quad y_{l_i(j+1)} < y_{l_i} < y_{l_i(j+2)}; \\ \vdots & \vdots \qquad \vdots \\ \sum_{l_1=0}^{m}\cdots\sum_{l_n=0}^{m} c_{(j+k)l} z^{-1} y_{l_1}\cdots z^{-1} y_{l_n} & \text{if} \quad y_{l_i(j+k-1)} < y_{l_i} < y_{l_i(j+k)}. \end{cases} \right), \quad i = 1,\ldots,n, \qquad (18)$$

here $f_i^{-1}(.)$ is the solution of the equation

ISSN 2086-8138 (print) | 2745-7249 (online) Vol. 15, No. 1, January 2021, pp. 56-67

$$z^{-1}y_i+\frac{T}{2}\begin{cases}\sum_{l_1=0}^{m}\cdots\sum_{l_n=0}^{m}c_{jl}z^{-1}y_{l_1}\cdots z^{-1}y_{l_n} & if \quad y_{l_i j}<y_{l_i}<y_{l_i(j+1)};\\ \sum_{l_1=0}^{m}\cdots\sum_{l_n=0}^{m}c_{(j+1)l}z^{-1}y_{l_1}\cdots z^{-1}y_{l_n} & if \quad y_{l_i(j+1)}<y_{l_i}<y_{l_i(j+2)};\\ \vdots & \vdots \qquad \vdots\\ \sum_{l_1=0}^{m}\cdots\sum_{l_n=0}^{m}c_{(j+k)l}z^{-1}y_{l_1}\cdots z^{-1}y_{l_n} & if \quad y_{l_i(j+k-1)}<y_{l_i}<y_{l_i(j+k)}.\end{cases}=0, \tag{19}$$

for $z^{-1}y_i$.

It is clear that (17) and (18) define the dynamic of n-th order object in various time domains, and it is easy to increase the order of the (19) by considering its state variable as vectors in some hyperspace.

Since we use polynomials, which are defined with multiplication and sum operations, defining the vectors mentioned above is complex and hypercomplex spaces because sum and multiplication are defined for various complex variables. In this case, we can use state variables' real and imaginary values as new state variables, which have clearly defined interrelations between them. Moreover, approximation terms can be complex too. This possibility allows us to make object dynamics more complex without considering any complex nonlinear functions. If one uses well-known complex and hypercomplex numbers, he finds that the resulting object's order is increased as 2n times. Simultaneously, if one defines own complex algebra, he can use complex variables of any order.

Let us show the proposed approach for increasing the complexity of objects with chaotic dynamics.

3. Results and Discussion

Let us consider the well-known Mackey-Glass chaotic system [38]. This system in operator form is described by following differential equation (20).

$$sy=-y+2\frac{y\,exp(-\tau s)}{1+\left(y\,exp(-\tau s)\right)^{10}} \tag{20}$$

here y_τ is a state variable value backward shifted on τ sec.

The considered system is the first order dynamical system with a single variable nonlinear second summand in its right-hand differential equation. Thus, this system can be used as a single-channel chaotic generator in secured communications.

We take into account the fact that shift operator $exp(-\tau s)$ in the time domain can be approximated as (21).

$$exp(-\tau s)=z^{-\tau/T} \tag{21}$$

and apply to (20) Tastin transformation (5) to be able to implement with system in discrete time domain by using microcontroller devices. Results of transformation is represented like (9).

$$y=\frac{(2-T)z^{-1}y+\dfrac{2Tz^{-\frac{\tau}{T}-1}y}{1+\left(z^{-\frac{\tau}{T}-1}y\right)^{10}}+\dfrac{2Tz^{-\frac{\tau}{T}}y}{1+\left(z^{-\frac{\tau}{T}}y\right)^{10}}}{2+T} \tag{22}$$

We call (22) as discrete time model for Mackey-Glass chaotic generator.

Vol. 15, No. 1, January 2021, pp. 56-67 ISSN 2086-8138 (print) | 2745-7249 (online)

This model has two highly nonlinear summands. These summands depend on the shifted output signal—the number of shifted samples defined by lag time τ and sample time T.

Now we transform these summands into piecewise form by using cubic spline piecewise approximation. The transformation routine can be simplified by using MatLab Curve Fitting Toolbox. This toolbox uses various least square methods to minimize cost function (14). One can see the results of the approximation in Fig.1. Analysis of the approximation characteristics RMSE, SSE, and R-squares show high accuracy of the performed approximation.

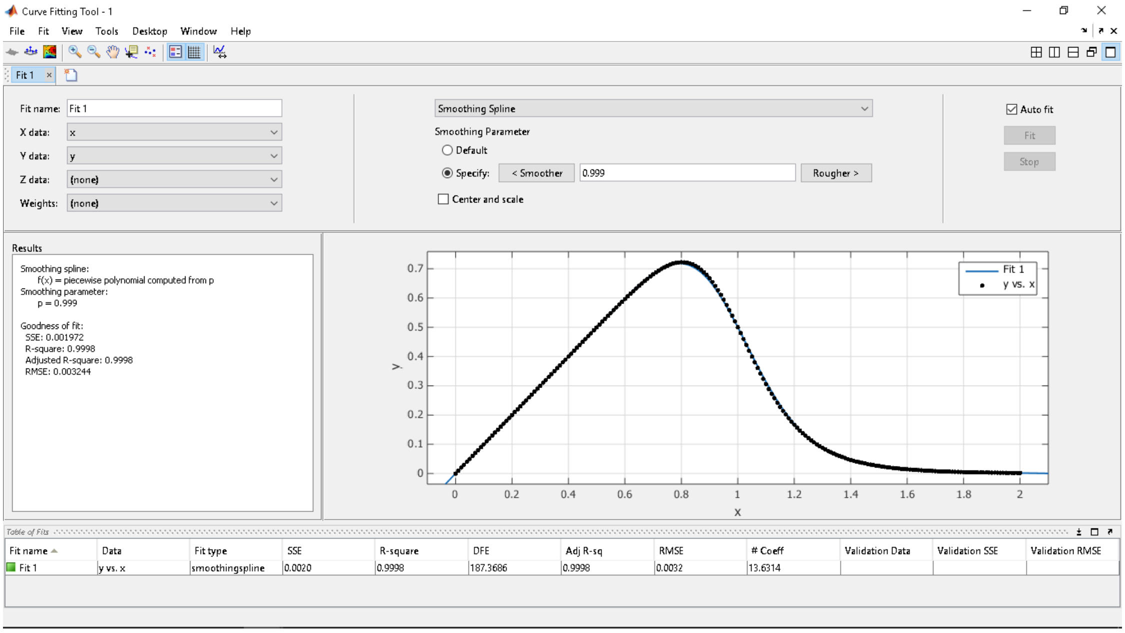

Fig. 1. Approximation of nonlinear summand by cubic spline

As a result of approximation nonlinear summands in (20) replaced with cubic splines as follows

$$\frac{y}{1+y^{10}} = \begin{cases} c_{13}y^3 + c_{12}y^2 + c_{11}y + c_{10} & if \quad 0 < y < 0.2; \\ \vdots & \vdots \quad\quad \vdots \\ c_{m3}y^3 + c_{m2}y^2 + c_{m1}y + c_{m0} & if \quad 1.8 < y < 2.0, \end{cases} \tag{23}$$

and the spline terms c_{ij} and breakpoints are defined. One can find these terms in Table 1.

Table 1. Spline terms and breakpoints

Breakpoint number i	Spline Terms				Breakpoint
	c_{i3}	c_{i2}	c_{i1}	c_{i0}	
1	-0.0844	0.0506	-0.0221	0.005	2
2	-0.3708	0.2731	0.0868	0.0144	1.8
3	-0.4682	0.5540	-0.2522	0.0464	1.6
4	-6.0944	4.2106	-1.2051	0.1678	1.4
5	9.6729	-1.5931	-1.7286	0.48999	1.2
6	7.5666	-6.1331	-0.1834	0.71	1.0
7	-10.5448	-0.1938	1.0045	0.5971	0.8
8	-0.5001	-0.1062	0.9870	0.3999	0.6
9	-0.2177	0.0243	1.0033	0.20000	0.4
10	0.0406	0	0.9985	0	0.2

Expression (23) gives us possibility to rewrite (22) in cubic spline form for i-th interval.

$$y_i = \frac{2-T}{2+T} z^{-1} y_i + \frac{2T}{2+T}\left(c_{i3}y_i^3 + c_{i2}y_i^2 + c_{i1}y_i + c_{i0}\right)\left(z^{-\frac{\tau}{T}-1} + z^{-\frac{\tau}{T}}\right) \tag{24}$$

ISSN 2086-8138 (print) | 2745-7249 (online) Vol. 15, No. 1, January 2021, pp. 56-67

Thus, the initial discrete-time chaotic generator is replaced with a similar one, which operates according to the simpler algorithm. There is no need to use division operators and rise state variables into high power.

Simulation results for the chaotic system (24) are shown in Fig.2. We show simulation results for the initial system (22) in this figure as well.

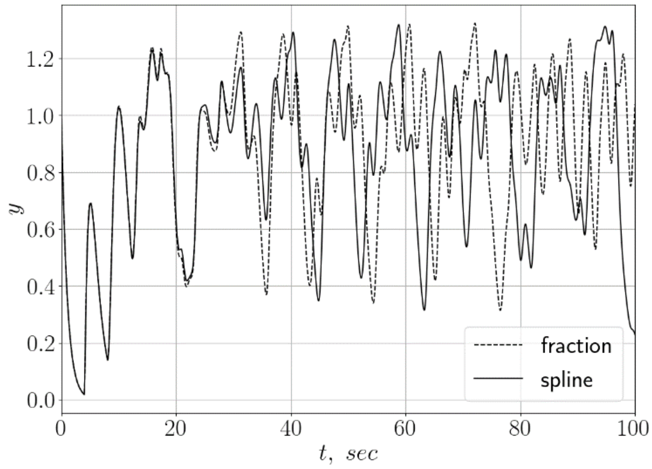

Fig. 2. Simulation results for the initial and the designed systems

Analysis of the simulation results shows that due to high approximation accuracy in the time interval from systems start to 15 s produced chaotic oscillations a very close in both systems after 15s deviation between the systems occurs. After 25 s, this deviation becomes significant, and both systems produce different oscillations. Moreover, piecewise systems produce chaotic oscillations with the Lyapunov exponents, which are 0.0883,- 0.0146, -0.0294, -0.1468, and the initial nonlinear system following Lyapunov exponents 0.0464, 0.01351, -0.0165, -0.0549. Since the greatest Lyapunov exponents are positive, we can predict chaos occurring. Moreover, the highest Lyapunov exponent in the designed system is greater than in the initial one. Thus, one can conclude that piecewise chaotic systems produce more unpredictable oscillations.

This fact allows claiming that piecewise approximation of nonlinear functions in the considered dynamical system makes it possible to construct similar, chaotic systems. Different chaotic oscillations will be generated if these systems even slightly differ by approximation terms and breakpoints. It is a possible method to make system dynamics more unpredictable and save transmitted data from interception and decryption.

The second method to improve system performance is defining multichannel system dynamics by using vectors instead of scalar. One can use complex and hypercomplex numbers to perform calculations with vectors in the 2D plane and the N-th dimensional space.

However, the piecewise expression's main feature (23) and similar to it is the comparison current function argument with breakpoints coordinate. This comparison is trivial for the scalar system and non-trivial for vector ones because no vector compares operations.

To avoid this drawback, we use both components of a complex number to represent (23) in the complex plane as follows

$$\frac{y}{1+y^{10}}=\begin{cases} c_{13}\,Re\left(y^3\right)+c_{12}\,Re\left(y^2\right)+c_{11}\,Re\left(y\right)+c_{10}+ & \text{if} \quad 0<Re(y)<0.2; \\ +jc_{13}\,Im\left(y^3\right)+jc_{12}\,Im\left(y^2\right)+jc_{11}\,Im\left(y\right)+jc_{10} & \quad\quad 0<Im(y)<0.2 \\ \vdots & \vdots \quad\quad \vdots \\ c_{m3}\,Re\left(y^3\right)+c_{m2}\,Re\left(y^2\right)+c_{m1}\,Re\left(y\right)+c_{m0}+ & \text{if} \quad 1.8<Re(y)<2.0; \\ +jc_{m3}\,Im\left(y^3\right)+jc_{m2}\,Im\left(y^2\right)+jc_{m1}\,Im\left(y\right)+jc_{m0} & \quad\quad 1.8<Im(y)<2.0, \end{cases} \tag{25}$$

here j is an imaginary unit, Re(y) and Im(y) means real and imaginary parts of y variable.

Thus, one can generalize (25) and claim that it is necessary to compare each vector component with breakpoints in N-th dimensional space.

In this case, one can rewrite (24) as follows

$$\begin{pmatrix} Re\left(y_i\right)+ \\ +j\,Im\left(y_i\right) \end{pmatrix}=\frac{2-T}{2+T}\begin{pmatrix} Re\left(z^{-1}y_i\right)+ \\ +j\,Im\left(z^{-1}y_i\right) \end{pmatrix}+\frac{2T}{2+T}\begin{pmatrix} c_{i3}\,Re\left(y_i^3\right)+c_{i2}\,Re\left(y_i^2\right)+c_{i1}Re\left(y_i\right)+c_{i0}+ \\ +jc_{i3}\,Im\left(y_i^3\right)+jc_{i2}\,Im\left(y_i^2\right)+jc_{i1}\,Im\left(y_i\right)+jc_{i0} \end{pmatrix}\left(z^{-\frac{\tau}{T}-1}+z^{-\frac{\tau}{T}}\right) \tag{26}$$

The result of a numerical solution of (26) is shown in Fig.3. We use different initial conditions for real and imaginary parts of state variable y to get different oscillations.

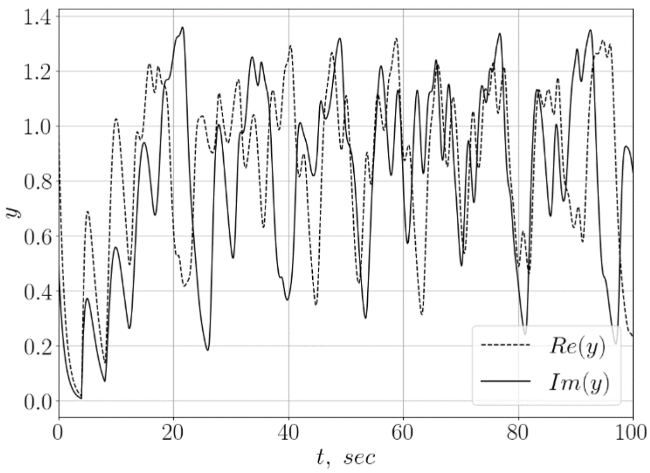

Fig. 3. Chaotic oscillations in dual channel Mackey-Glass system with cubic splines

The highest Lyapunov exponents for these oscillations are 0.0883 and 0.0827, and these numbers are greater than the exponent value for the initial system. Thus, the designed dual-channel chaotic system is the chaotic system with improved unpredictable features.

A designed chaotic system has two channels, and it is possible to use both of them to transmit data. Moreover, if necessary, these channels can be considered the basis to design other chaotic systems by using various linear and nonlinear combinations of signals Re(y) and Im(y). One such combination is the transformation of the complex number from algebraic into exponential form.

One more approach to increase encoding properties of the designed chaotic system is using complex weight terms. In this case, (27) can be represented as follows.

$$\begin{pmatrix} Re\left(y_i\right)+ \\ +j\,Im\left(y_i\right) \end{pmatrix}=k_1\begin{pmatrix} Re\left(z^{-1}y_i\right)+ \\ +j\,Im\left(z^{-1}y_i\right) \end{pmatrix}+k_2\left(\alpha+j\beta\right)\begin{pmatrix} c_{i3}\,Re\left(y_i^3\right)+c_{i2}\,Re\left(y_i^2\right)+c_{i1}Re\left(y_i\right)+c_{i0}+ \\ +jc_{i3}\,Im\left(y_i^3\right)+jc_{i2}\,Im\left(y_i^2\right)+jc_{i1}\,Im\left(y_i\right)+jc_{i0} \end{pmatrix}\left(z^{-\frac{\tau}{T}-1}+z^{-\frac{\tau}{T}}\right), \tag{27}$$

Where the k-condition can be calculated with (28).

$$k_1=\frac{2-T}{2+T};k_2=\frac{2T}{2+T} \tag{28}$$

ISSN 2086-8138 (print) | 2745-7249 (online)
Vol. 15, No. 1, January 2021, pp. 56-67

For example, if one assume $\alpha = 1, \beta = 0.3$, he can get following simulation results on Fig. 4.

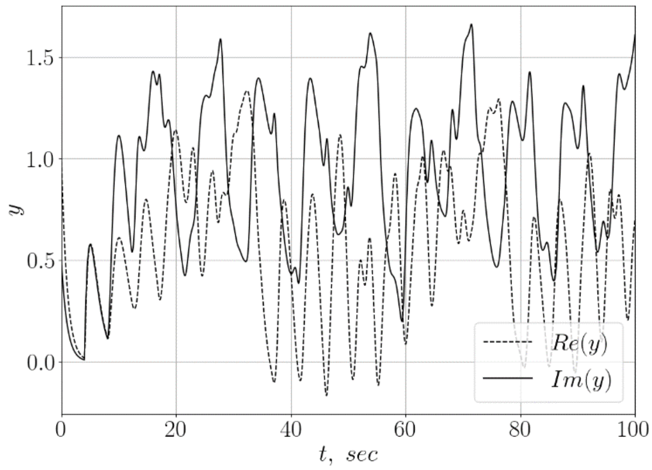

Fig. 4. Simulation results for a dual chaotic system with cross-connections between real and imaginary channels

The greatest Lyapunov exponents, in this case, are 0.0832 and 0.0954. These values conclude that the solution of (24) produces the most unpredictable oscillations among the considered systems.

4. Conclusion

The cubic spline approximation allows us to simplify the nonlinear dynamic system model and represent it in a less nonlinear form. If one applies the transformation of the continuous chaotic system into discrete-time, he can build the model, which can be used to implement this model on various digital devices. This implementation is performed by using sets of the third-order polynomials and if … then… conditional operators. These operators spend quite a lot of processor time, so the number of breakpoints should be minimal to obtain the desired approximation accuracy. For example, the use of 20 if...then… construction and cubic polynomials, while PC simulating has increased calculation time by 44% compared to the initial nonlinear system, and reducing conditional constructions to 2, allows us to get the same simulation time in both systems. It is possible to increase chaotic system order and produce more unpredictable chaotic oscillations by using complex and hypercomplex numbers. These numbers define chaotic multichannel systems. One can use these channels to transmit data or apply some algebraic transformations for these signals to improve chaotic transmission security.

Declarations

Author contribution. All authors contributed equally to the main contributor to this paper. All authors read and approved the final paper.
Funding statement. None of the authors have received any funding or grants from any institution or funding body for the research.
Conflict of interest. The authors declare no conflict of interest.
Additional information. No additional information is available for this paper.

References

[1] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, "Handbook of Applied Cryptography CRC Press," *Boca Rat.*, 1997, [Online]. Available: Google Scholar.

[2] C. E. Shannon, "Claude Elwood Shannon: Collected Papers," 1993, [Online]. Available: https://dl.acm.org/doi/book/10.5555/174843.

[3] C. E. Shannon, "A Mathematical Theory of Communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, Jul.

1948, doi: 10.1002/j.1538-7305.1948.tb01338.x.

[4] G. A. Jones and J. Mary Jones, "Information and Coding Theory," 2000, doi: 10.1007/978-1-4471-0361-5.

[5] D. Coppersmith, "The Data Encryption Standard (DES) and its strength against attacks," *IBM J. Res. Dev.*, vol. 38, no. 3, pp. 243–250, May 1994, doi: 10.1147/rd.383.0243.

[6] M. W. Hirsch, S. Smale, and R. L. Devaney, "Differential Equations, Dynamical Systems, and an Introduction to Chaos," 2013, doi: 10.1016/C2009-0-61160-0.

[7] G. C. Layek, "An Introduction to Dynamical Systems and Chaos," 2015, doi: 10.1007/978-81-322-2556-0.

[8] N. Swarupa, "Design and Simulation of Chaotic Colpitt's Oscillator," *2018 Second Int. Conf. Electron. Commun. Aerosp. Technol.*, pp. 1505–1508, Mar. 2018, doi: 10.1109/ICECA.2018.8474857.

[9] C. Wannaboon and T. Masayoshi, "An autonomous chaotic oscillator based on hyperbolic tangent nonlinearity," *2015 15th Int. Symp. Commun. Inf. Technol.*, pp. 323–326, Oct. 2015, doi: 10.1109/ISCIT.2015.7458372.

[10] T. Xie, X. Wei, and R. Yu, "Noise Immunity Analysis in External Excitation Chaotic Oscillator Detecting System," *2010 Int. Conf. Intell. Syst. Des. Eng. Appl.*, pp. 1013–1016, Oct. 2010, doi: 10.1109/ISDEA.2010.154.

[11] E. V Efremova, A. Y. Nikishov, and A. I. Panas, "UWB microwave chaotic oscillator: From distributed structure to CMOS IC realization," *Proc. Pap. 5th Eur. Conf. Circuits Syst. Commun.*, pp. 67–70, 2010, [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5733858.

[12] S. Hu, S. Yu, Y. Hu, Z. Wang, and B. Zhou, "A Novel 1–6 GHz Chaotic Signal Oscillator for Broadband Communication Systems," *2018 Prog. Electromagn. Res. Symp.*, pp. 1550–1554, Aug. 2018, doi: 10.23919/PIERS.2018.8598177.

[13] A. Semenov, O. Osadchuk, O. Semenova, O. Bisikalo, O. Vasilevskyi, and O. Voznyak, "Signal Statistic and Informational Parameters of Deterministic Chaos Transistor Oscillators for Infocommunication Systems," *2018 Int. Sci. Conf. Probl. Infocommunications. Sci. Technol. (PIC S&T)*, pp. 730–734, Oct. 2018, doi: 10.1109/INFOCOMMST.2018.8632046.

[14] S. Ergun, "Cryptanalysis of a random number generator based on a double-scroll chaotic oscillator," *2016 Int. Symp. Intell. Signal Process. Commun. Syst.*, pp. 1–4, Oct. 2016, doi: 10.1109/ISPACS.2016.7824723.

[15] M. Moundher, B. Hichem, T. Djamel, and S. Said, "Novel Four-dimensional Chaotic Oscillator for Sub-1GHz Chaos-Based Communication Systems," *2019 6th Int. Conf. Image Signal Process. their Appl.*, pp. 1–5, Nov. 2019, doi: 10.1109/ISPA48434.2019.8966791.

[16] K. Klomkarn and P. Sooraksa, "A Universal-Mode Chaotic Oscillator," *2019 Jt. Int. Conf. Digit. Arts, Media Technol. with ECTI North. Sect. Conf. Electr. Electron. Comput. Telecommun. Eng. (ECTI DAMT-NCON)*, pp. 314–317, Jan. 2019, doi: 10.1109/ECTI-NCON.2019.8692295.

[17] M. Tabatabaei, J. Zarei, R. Razavi-Far, and M. Saif, "Secure Communication Based on Fractional Chaotic System by a Novel Robust Filter Algorithm," *2020 IEEE Int. Syst. Conf.*, pp. 1–6, Aug. 2020, doi: 10.1109/SysCon47679.2020.9275914.

[18] J. Kim, B. Van Nguyen, H. Jung, J.-H. Lee, and K. Kim, "A Novel Chaotic Time Hopping TH-NRDCSK System for Anti-jamming Communications," *2019 IEEE Wirel. Commun. Netw. Conf.*, pp. 1–3, Apr. 2019, doi: 10.1109/WCNC.2019.8885532.

[19] S. A. R. F. M. Nejad and A. Sahab, "A novel 5-D hyper-chaotic system with single equilibrium point and designing a controller for it using the optimal generalized back-stepping method," *2017 IEEE Int. Conf. Cybern. Comput. Intell.*, pp. 29–33, Nov. 2017, doi: 10.1109/CYBERNETICSCOM.2017.8311710.

[20] L.-M. Tam and S.-Y. Li, "Novel-fuzzy-model based modeling and control of nonlinear chaotic systems with uncertainty," *2015 Int. Conf. Adv. Robot. Intell. Syst.*, pp. 1–6, May 2015, doi: 10.1109/ARIS.2015.7158361.

[21] H. Deng, T. Li, Q. Wang, and H. Li, "A Novel Chaotic Slow FH System Based on Differential Space-Time Modulation," *2008 Int. Conf. Embed. Softw. Syst. Symp.*, pp. 380–385, Jul. 2008, doi: 10.1109/ICESS.Symposia.2008.71.

[22] R. Voliansky, O. Kluev, O. Sadovoi, O. Sinkevych, and N. Volianska, "Chaotic Time-variant Dynamical System," *2020 IEEE 15th Int. Conf. Adv. Trends Radioelectron. Telecommun. Comput. Eng.*, pp. 606–609, Feb. 2020, doi: 10.1109/TCSET49122.2020.235503.

[23] R. Voliansky, A. Pranolo, A. P. Wibawa, and Haviluddin, "Transformation of 3-D Jerk Chaotic System into Parallel Form," *2018 Int. Symp. Adv. Intell. Informatics*, pp. 179–184, Aug. 2018, doi: 10.1109/SAIN.2018.8673346.

[24] H. Chen, L. Wu, L.-D. Lin, G.-Q. Lan, and Q. Ding, "Simulation Experiment Research on the Chaotic Characteristics of the Simple Unary Polynomial Transformation," *2012 Fifth Int. Work. Chaos-fractals Theor. Appl.*, pp. 118–122, Oct. 2012, doi: 10.1109/IWCFTA.2012.34.

[25] Z. Zhu, S. Li, H. Yu, X. Liu, and J. Song, "An approach of chaotic generalized synchronization with the space transformation," *2008 IEEE Int. Symp. Ind. Electron.*, pp. 1088–1092, Jun. 2008, doi: 10.1109/ISIE.2008.4676930.

[26] H. Chen, M. Gao, and H. Zhang, "Study Chaotic Sequences by Unary Quadratic Nonlinear Transformation," *2011 Fourth Int. Work. Chaos-Fractals Theor. Appl.*, pp. 169–173, Oct. 2011, doi: 10.1109/IWCFTA.2011.17.

[27] R. Voliansky, O. Sadovoi, Y. Shramko, N. Volianska, and O. Sinkevych, "Arduino-based Implementation of the Dual-channel Chaotic Generator," *2019 3rd Int. Conf. Adv. Inf. Commun. Technol.*, pp. 278–281, Jul. 2019, doi: 10.1109/AIACT.2019.8847904.

[28] M. Jalilian, A. Ahmadi, and M. Ahmadi, "Hardware Implementation of A Chaotic Pseudo Random Number Generator Based on 3D Chaotic System without Equilibrium," *2018 25th IEEE Int. Conf. Electron. Circuits Syst.*, pp. 741–744, Dec. 2018, doi: 10.1109/ICECS.2018.8617960.

[29] H. Zheng, S. Yu, and J. Lu, "Multi-images chaotic communication and FPGA implementation," *Proc. 33rd Chinese Control Conf.*, pp. 5481–5485, Jul. 2014, doi: 10.1109/ChiCC.2014.6895876.

[30] S. Liu, "Research on the design and implementation of two dimensional hyper chaotic sequence cipher algorithm," *2017 Sixth Int. Conf. Futur. Gener. Commun. Technol.*, pp. 1–4, Aug. 2017, doi: 10.1109/FGCT.2017.8103730.

[31] S. Liu, "Research on the Design and Implementation of Two Dimensional Hyper Chaotic Sequence Cipher Algorithm," *2017 Int. Conf. Comput. Syst. Electron. Control*, pp. 1185–1187, Dec. 2017, doi: 10.1109/ICCSEC.2017.8446935.

[32] E. Huesca and S. Mondie, "Lyapunov matrix of linear systems with delays: A polynomial approximation," *2009 6th Int. Conf. Electr. Eng. Comput. Sci. Autom. Control*, pp. 1–6, Nov. 2009, doi: 10.1109/ICEEE.2009.5393438.

[33] A. Krifa and K. Bouzrara, "Approximation of nonlinear term in model robotic," *2017 Int. Conf. Control. Autom. Diagnosis*, pp. 185–190, Jan. 2017, doi: 10.1109/CADIAG.2017.8075654.

[34] D. Babic, "Piecewise polynomial approximation based on taylor series with efficient realization using Farrow structure," *2009 9th Int. Conf. Telecommun. Mod. Satell. Cable, Broadcast. Serv.*, pp. 241–244, Oct. 2009, doi: 10.1109/TELSKS.2009.5339415.

[35] C. Lubich, D. Mansour, and C. Venkataraman, "Backward difference time discretization of parabolic differential equations on evolving surfaces," *IMA J. Numer. Anal.*, vol. 33, no. 4, pp. 1365–1385, Oct. 2013, doi: 10.1093/imanum/drs044.

[36] K. B. Janiszowski, "A modification and the Tustin approximation," *IEEE Trans. Automat. Contr.*, vol. 38, no. 8, pp. 1313–1316, 1993, doi: 10.1109/9.233177.

[37] Jang-Ho Seo, Chang-Hwan Im, Chang-Geun Heo, Jae-Kwang Kim, Hyun-Kyo Jung, and Cheol-Gyun Lee, "Multimodal function optimization based on particle swarm optimization," *IEEE Trans. Magn.*, vol. 42, no. 4, pp. 1095–1098, Apr. 2006, doi: 10.1109/TMAG.2006.871568.

[38] P. Amil, C. Cabeza, and A. C. Marti, "Exact Discrete-Time Implementation of the Mackey–Glass Delayed Model," *IEEE Trans. Circuits Syst. II Express Briefs*, vol. 62, no. 7, pp. 681–685, Jul. 2015, doi: 10.1109/TCSII.2015.2415651.