AUTOMATIC CONTROL SYSTEMS

UDC 681.51:519.7(045)
DOI: 10.18372/1990-5548.59.13636

[1]V. V. Kyrychenko,
[2]Ye. V. Lesina

EFFECT OF DYNAMIC DEGRADATION IN ALGORITHMS FOR DATA SECURITY

[1]Department of Machine dynamics and strength of materials, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
[2]Department of Automatics and Telecommunications, Donetsk National Technical University, Pokrovsk, Ukraine
E-mails: [1]vkir28@gmail.com, [2]eugenia.lesina@donntu.edu.ua

***Abstract*—*The algorithm of data encryption using discrete chaotic systems and transformations is considered. The features of reversible discrete control systems as information transformers are studied, in particular, such a property as dynamic degradation. It consists in the possible sharp decrease of a discrete set of states of a complex dynamic system with the introduction of an information message. To a large extent, this phenomenon depends on the initial values of the trajectories and parameters of the system. An example of a dynamic system whose trajectories have a complex internal dynamic is given, but when an information message is introduced into it, they fall on a zero invariant manifold. Thus, instead of encrypting the input information sequence, the output of the system for any values of key parameters, starting from a certain moment, accurately transmits the value of the information input with a unit delay.*

Index Terms—Inverse dynamic systems; dynamic degradation; ring of integers; encryption; control function.

I. INTRODUCTION

In connection with the development of information communication systems, the importance of the problem of confidentiality of information transfer and the broader problem of protecting information in the communications services market is increasing. Nowadays, there is an urgent need to protect commercial information in computer networks, ensure the security of electronic payments, Internet telephony and so on. A typical requirement is the need for mass application of coding algorithms and their low cost per unit of "informational" products.

Along with traditional encryption algorithms that are constantly being developed and improved, encryption algorithms based on dynamic chaos systems are becoming increasingly popular in the cryptographic community.

Dynamic chaos systems are dynamic systems with an exponential state dependence on initial conditions, i.e. a small change in the initial state of the system leads to a significant change in the entire trajectory of the system on the phase plane. The change in initial conditions increases exponentially with time.

The problem of study about possibilities of usage chaotic systems in communication technologies, development and approbation of concrete algorithms set and chaotic encryption schemes, which provide the controlled degree of privacy, is becoming an actual problem. These schemes must provide: a) high effectiveness of protecting multimedia information; b) high encryption velocity; c) high stability according to noise. In solving problem of protecting information, the methodic, based on determined chaos, which is generated by nonlinear dynamic systems, can be successfully used. However, it needs to determine the following properties of dynamic systems, which provide possibilities of their usage.

The basis for such systems is the property of reversibility, that is, the ability to restore the external input (informational message) of a nonlinear dynamic system with regard to its output (a signal that is sent to the communication networks). The phenomenon of reversibility is widely used in many problems of the theory of control of complex systems.

The proof of the fact of randomness of the trajectories for a given dynamic system is a complex mathematical problem.

II. REVIEW OF RESEARCHES

Recently, with the advent of [1], the possibilities of using dynamic systems that have a chaotic behavior in telecommunication technologies ([2], [3], [4]) have been intensively studied.

Separately, we would like to dwell on the works of Yu. V. Andreev, A. S. Dmitriev, and others [5], [6], who consider the role of dynamic chaos in information processing in nonlinear systems. This group of authors put forward a hypothesis about the existence of general principles of information processing in systems with complex dynamics independent of the implementation of the systems themselves. On its basis, they consider the possibility of constructing relatively simple mathematical structures (one-dimensional and multi-dimensional mappings of a special type). Those implement various information processing processes using deterministic chaos.

Computer implementation of information conversion algorithms based on dynamic systems, which have the above properties, leads to the need for discretization of such systems. Therefore, it becomes relevant to study the information characteristics of discrete computer implementations of coding algorithms (statistical properties, recognition of constant sequences of characters, alphabet size, influence of interference), as well as coding algorithms that use the properties of dynamic systems with chaotic behavior. This problem is studied, for example, in [7].

III. Problem Statement

The schemes of determined of unknown input by information about system output, which are true for continuous systems, can be used also for discrete system. The dynamics can be defined by the following equations:

$$x(k+1)=f(x(k),u(k)), \quad y(k)=h(x(k)). \qquad (1)$$

The output signal is transmitted via communication channels – a function $y(k)$, depending on the state of the system, its parameters and the message $u(k)$. To construct equations describing the dynamics of the receiving device, we consider the problem of recovering the values of the input action from the values of the output function. One way to solve it is to build a system inverse to the original one. In this case, the input information sequence $u(t)$ is fed to the input of the dynamic system, and the output $y(t)$ may not depend explicitly on $u(t)$. In this case, system (1) generates a unique input-output mapping.

System (1) is nonlinear, and its trajectories have rather complex behaviour. The exceptions are trajectories lying on invariant sets. In the general case, trajectories, hitting invariant sets, remain on it at all subsequent moments, which leads to a drop in the dimension of the phase space of the system states. The main purpose of this work is to study this situation when the system is used to encrypt data.

IV. Features of Discrete Control Systems

In the system (1) the output doesn't depend directly on input information sequence $u(k)$. Let's by analogy define the term of relative order input for continuous case. The function value $h(f(x,u))$ may not depend on values u, so similarly

$$y(k+1)=h(f(x(k),u(k)))$$

may not contain $u(k)$. Defining what is the delay of steps between input and output system (1). This value points at relative sequence input in system (1). Put

$$f^{i}(x,u)=f\circ f\cdots\circ f(x,u),\, i\geq 1,$$

where $\circ$ denotes function superposition. Let's say that system (1) has relative order $r>0$, if for each x,u

$$\frac{\partial(h\circ f^{i}(x,u))}{\partial u}\equiv 0,\, i=1,\ldots,r-1,$$

$$\frac{\partial(h\circ f^{r}(x,u))}{\partial u}\neq 0.$$

So, the relative order r for discrete system points at number of output sequence element, on which the first element of input sequence $u(0)$ directly influences. The substitution

$$\begin{pmatrix}\xi\\ \eta\end{pmatrix}=\begin{pmatrix}f^{r}(x)\\ \Phi(x)\end{pmatrix}, \quad \det\frac{\partial(f^{r}(x),\Phi(x))}{\partial x}\neq 0,$$

transforms the system (1) to the normal form

$$\begin{cases}\xi_i(k+1)=\xi_{i+1}(k),\\ \xi_r(k+1)=F(\xi(k),\eta(k),u(k)),\\ \eta\,(k+1)=G(\xi(k),\eta(k),u(k)), \quad i=1,\ldots,r,\end{cases} \qquad (2)$$

where, like in continuous case, ξ,η denote internal and external dynamics respectively. Solving equation relative $u(k)$

$$\xi_r(k+1)=F\left(\xi(k),\eta(k),u(k)\right),$$

find

$$u(k)=g(\xi_r(k+1),\xi(k),\eta(k)). \qquad (3)$$

After substitution (3) in (2) get inverse discrete dynamic system

$$\eta(k+1)=G(\xi_r(k+1),\,\xi(k),\,\eta(k)). \qquad (4)$$

Thus, for message restoring for given sequence $u(k)$, it's necessary to have information about $n-r$ initial conditions $\eta(0)$ of dynamic system (4) additionally to signal values $\xi_1(k),\ldots,\xi_r(k)$, $\xi_r(k+1)$. So for dynamic systems that are presented in discrete form, can be used algorithms discovered for continuous system. The modification is accounted for replacing derivative values from signal on corresponding output value of discrete system, received with delay, which is equal to derivative order.

V. Stability of Algorithms of Decription to Signal Errors

Let's consider discrete realization of described dynamic system and set a problem to determine their characteristics as data-flow dynamic encryption of information sequence $\{u(k), k=1,\dots N\}$. The transition to the operations in integer field allows to remove a number of difficulties, which appeared when using discrete dynamic systems. The general problem is connected with fact that usage of multidimensional systems leads to superfluous calculations. When using machine arithmetic with floating point, the redundancy of computational operations over data array leads to: a) obvious growth of data process time; b) fast growth of computation error.

The computing device with fixed point provides much more speed of calculations without errors. Besides, such computing devices can be easily realized in the form of digital encryptor-decryptor, located in the places of input and output of flow data information system to general communication net.

Examine one-dimensional discrete system, the right sides of which don't depend on internal influence (the system modulation absence by information signal $u(k)$):

$$x(k+1)=F\big(x(k)\big)$$

Let the machine accuracy of computing device, that is used, is *L* bits. Then, any value *A* is represented in binary code, has the view *A* mod 2*L*. It means that values *A* are included in set {0, 1, 2, …, 2*L* – 1}. Following to that measure integer-valued points in space R^n is equal to zero, the dynamic system, is written in finite field with 2*L* elements, cannot valid describe dynamics of chaotic system, that caused it.

The next conclusion is the result of determinacy and the fact that state space *x*(*k*) is determined by 2*L* values {0, 1, 2, …, 2*L* – 1}:

Any system trajectory with initial condition *x*(0) in the field of integers in modulus 2*L* will be periodic with period *TX*(0), as a rule less than 2*L*. Therefore, one of the criterion of chaotic dynamic system – continuous spectrum of solutions – is not fulfilled. Integer-valued trajectory has discrete spectrum divisible by *TX*(0).

So, for the dynamic system in the field of integers in modulus *2L* the chaotic masking method, where the signal, that is transferred, carries information in the form $y(k)=x(k)+u(k)$, doesn't change frequency properties of message $u(k)$.

VI. Results of Experimental Researches

The quantity of different states phase vector *x*(*k*) in case of *n*-dimensional system increases to 2*L*·*n*. Computer generated simulation of encrypting-decrypting process by described scheme shows that at some initial conditions and system parameters (which significantly differ from initial transmitter's state) large informational arrays can be restored with the aid of given inverse system and approximately without distortions. This fact is undesirable effect because of decreasing cryptographic quality encrypted scheme.

The effect of regression own system dynamics at entering to right part non-autonomous disturbance, is called dynamic degradation.

For examination this effect let's analyze the following example. Suppose that transmitter (encryptor) is formed by the base of Euler's equations, that describe motion of solid body, and construct appropriate inverse system [6]. For discovering degradation effect let adjust special transmitter's parameters: the coefficients in the right-hand side are equal to one, output will be second coordinate. So, have nonlinear input-output system, where to input is applied message $u(k)$:

$$\begin{aligned}&x_1(k+1)=x_2(k)\cdot x_3(k)\bmod 2L,\\&x_2(k+1)=x_1(k)\cdot x_3(k)+u(k)\bmod 2L,\\&x_3(k+1)=x_1(k)\cdot x_2(k)\bmod 2L,\end{aligned}\tag{5}$$

$$y(k)=x_2(k).$$

Signal $y(k)$ is directed to communication net. The unknown initial system conditions $x_1(0), x_2(0), x_3(0)$ are decryption key. The receiver (decryptor) is inverse system with the aid of which are realized restoring values $u(k)$, when keys are known, using formulas:

$$\begin{aligned}&x_1(k+1)=x_2(k)\cdot x_3(k)\bmod 2L,\\&x_2(k+1)=y(k+1),\\&x_3(k+1)=x_1(k)\cdot x_2(k)\bmod 2L,\\&u(k)=y(k+1)-x_1(k)\cdot x_3(k)\bmod 2L.\end{aligned}$$

Write first iterations of signal values $k=0,1,2,3,4,5,6$:

$$\begin{aligned}&y(0)=x_2(0),\\&y(1)=x_1(0)x_3(0)+u(0),\\&y(2)=x_1(1)x_3(1)+u(1)=x_2^2(0)x_1(0)x_3(0)+u(1),\end{aligned}$$

$$y(3)=x_1(2)x_3(2)+u(2)=\left[x_1(0)x_3(0)+u(0)\right]^2 x_1(1)x_3(1)+u(2)=\left[x_1(0)x_3(0)+u(0)\right]^2 x_2^2(0)x_1(0)x_3(0)+u(2),$$

$$\begin{aligned}y(4)=x_1(3)x_3(3)+u(3)&=\left[x_2^2(0)x_1(0)x_3(0)+u(1)\right]^2 x_1(2)x_3(2)+u(3)\\&=\left[x_2^2(0)x_1(0)x_3(0)+u(1)\right]^2\cdot\left[x_1(0)x_3(0)+u(0)\right]^2\cdot x_2^2(0)\cdot x_1(0)x_3(0)+u(3),\end{aligned}$$

$$\begin{aligned}y(5)=x_1(4)x_3(4)+u(4)&=\left[\left[x_1(0)x_3(0)+u(0)\right]^2 x_2^2(0)x_1(0)x_3(0)+u(2)\right]^2 x_1(3)x_3(3)+u(4)\\&=\left[\left[x_1(0)x_3(0)+u(0)\right]^2 x_2^2(0)x_1(0)x_3(0)+u(2)\right]^2\cdot\left[x_2^2(0)x_1(0)x_3(0)+u(1)\right]^2\\&\qquad\cdot\left[x_1(0)x_3(0)+u(0)\right]^2\cdot x_2^2(0)\cdot x_1(0)x_3(0)+u(4),\end{aligned}$$

$$\begin{aligned}&y(6)=x_1(5)x_3(5)+u(5)\\&=\left[\left[x_2^2(0)x_1(0)x_3(0)+u(1)\right]^2\cdot\left[x_1(0)x_3(0)+u(0)\right]^2\cdot x_2^2(0)\cdot x_1(0)x_3(0)+u(3)\right]^2 x_1(4)x_3(4)+u(5)\\&=\left[\left[x_2^2(0)x_1(0)x_3(0)+u(1)\right]^2\cdot\left[x_1(0)x_3(0)+u(0)\right]^2\cdot x_2^2(0)\cdot x_1(0)x_3(0)+u(3)\right]^2\\&\qquad\cdot\left[\left[x_1(0)x_3(0)+u(0)\right]^2 x_2^2(0)x_1(0)x_3(0)+u(2)\right]^2\cdot\left[x_2^2(0)x_1(0)x_3(0)+u(1)\right]^2\\&\qquad\cdot\left[x_1(0)x_3(0)+u(0)\right]^2\cdot x_2^2(0)\cdot x_1(0)x_3(0)+u(5).\end{aligned}$$

From the achieved formulas the recurrence relation for determination $u(k)$ is followed:

$$\begin{cases}y(0)=x_2(0),\\ y(1)=u(0)+x_1(0)x_3(0),\\ y(k)=u(k-1)+x_1(0)x_3(0)\prod\limits_{i=0}^{k-2}y^2(i), \quad k\ge 2.\end{cases}$$

This implies,

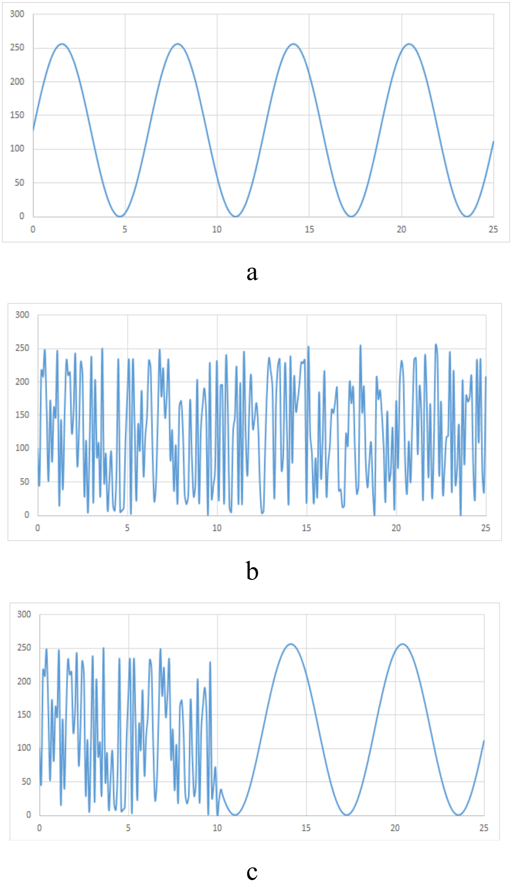
$$u(k-1)=\begin{cases}y(k)-x_1(0)x_3(0), \quad k=1,\\ y(k)-x_1(0)x_3(0)\prod\limits_{i=0}^{k-2}y^2(i), \quad k\ge 2.\end{cases}$$

The next confirmation for this problem takes place:

Confirmation: Suppose that for some integer N signal quantity of system (5) is $y(N)=x_1(N)x_3(N)+u(N)=0 \pmod{2L}$. Then for any $i>N+1$ $y(i)=u(i-1)$.

For demonstration this effect take function $u(x)=128\sin(x)+128$ (Fig. 1a) as input signal and encrypt with the help of system (6) when $L=128$.

The result of encrypting is shown on Fig. 1b. If at some step capture system value $u(x)$ in such manner that confirmation's condition is satisfied, then the degradation effect will take place (Fig. 1c).



a

b

c

Fig. 1. Periodic signal coding: (a) is the periodic signal; (b) is the without degradation effect; (c) is the with degradation effect

So, instead of encrypting informational sequence $u(k)$, the output of described dynamics system for any values of key parameters, starting from some moment, transmits input value with unit delay.

IV. Conclusion

One of the perspective direction of development contemporary telecommunication technologies is related with non-linear dynamics system, which possess chaotic behavior. Reversibility is the main feature for such systems. It means the opportunity to restore input influence (information message) by its output (signal), that are directed to communication net.

Computer algorithms realization of information transformation, which is based on chaotic dynamics, leads to necessity of system discretization. Examining specifics of inverse dynamics control systems as information transformers allowed experimentally detect degradation effect at some parameters values of dynamics systems. It consists in probable sudden decreasing discrete set of complex dynamics system states when entering information message. There is example of dynamics system, which trajectories have complex internal dynamic, but at entering information message make it into nonzero invariant manifold. Hereby, instead of encrypting input information sequence, the system output for any values of key parameters, starting from some moment, transmits input value with unit delay.

References

[1] M. J. Sobhy and A. Shehata, “Secure computer communication using chaotic algorithms,” *Int. J. of Bifurcation and Chaos*, vol. 10, no. 12, 2000, pp. 2831–2839.

[2] A. M. Kovalev, V. A. Kozlovsky, and V. F. Scsherbak, “Reversible dynamical systems with variable dimensionality of phase space in problems of cryptographic information transformation,” *Applied Discrete Mathematics*, no. 2(2), 2008, pp. 39–44.

[3] V. V. Kirichenko, “Information security of communication channel with UAV,” *Electronics and control systems*, no. 3 (45), 2015, pp. 23–27.

[4] V. V. Kyrychenko and Ye. V. Lesina, “Application of dynamic systems for encoding data in telecommunication channels,” *Electronics and control systems*, no. 3 (53), 2017, pp. 11–16. doi:10.18372/1990-5548.53.12137.

[5] A. S. Dmitriev, A. L. Panas, and S. O. Starkov, “Storing and recognition information based on stable cycles of one-dimensional maps,” *Phys. Lett. A.*, 1991, vol. 155.

[6] Yu.V. Andreev, A. S. Dmitriev and S. O. Starkov, “Information processing in 1-D systems with chaos,” *IEEE Transaction on circuit and systems*, 1997, vol. 44.

[7] V. V. Kyrychenko and Ye. V. Lesina, “Features of information UAV control system,” *Scientific papers of Donetsk National Technical University. Series: "Informatics, Cybernetics and Computer Science,"* no. 1(22), 2016, pp. 111–116.

Received September 12, 2018.

Kyrychenko Viktor. Candidate of Science (Physics and Mathematics).
Department of Machine Dynamics and Strength of Materials, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute,” Kyiv, Ukraine.
Education: Donetsk National University, Donetsk, Ukraine, (1999).
Research interests: gyroscopes theory, control systems and data processing.
Publications: 53.
E-mail: vkir28@gmail.com

Lesina Yevgeniya. Candidate of Science (Physics and Mathematics). Associate Professor.
Automatics and Telecommunications Department, Donetsk National Technical University, Pokrovsk, Ukraine.
Education: Donetsk National University, Donetsk, Ukraine, (2001).
Research interests: theory of differential equations, control systems and data processing.
Publications: 51.
E-mail: lesina17@gmail.com

В. В. Кириченко, Є. В. Лесіна. Ефект динамічної деградації в алгоритмах захисту даних

У роботі розглянуто особливості використання обернених дискретних динамічних систем управління в якості перетворювачів даних для передавання по телекомунікаційним каналам. Окремо виділено проблему динамічної деградації, яка полягає в можливому різкому зменшенні множини станів дискретної динамічної системи у разі надходження інформаційного сигналу на її вхід. В роботі наведено приклад такої системи, а також досліджено аналітично та чисельно ефект деградації, який виникає у разі її використання.

Ключові слова: зворотні динамічні системи; динамічна деградація; кільце цілих чисел; шифрування; функція контролю.

Кириченко Віктор Вікторович. Кандидат фізико-математичних наук.
Кафедра динаміки, міцності машин та опору матеріалів, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна.

Освіта: Донецький національний університет, Донецьк, Україна, (1999).
Напрямок наукової діяльності: теорія гіроскопів, системи управління та обробка інформації.
Кількість публікацій: 53.
E-mail: vkir28@gmail.com

Лесіна Євгенія Вікторівна. Кандидат фізико-математичних наук. Доцент.
Кафедра автоматики та телекомунікацій, Донецький національний технічний університет, Покровськ, Україна.
Освіта: Донецький національний університет, Донецьк, Україна, (2001).
Напрямок наукової діяльності: теорія диференціальних рівнянь, системи управління та обробка інформації.
Кількість публікацій: 51.
E-mail: eugenia.lesina@donntu.edu.ua

В. В. Кириченко, Е. В. Лесина. Эффект динамической деградации в алгоритмах защиты данных

В работе рассмотрены особенности использования обратных дискретных динамических систем управления в качестве преобразователей данных для передачи по телекоммуникационным каналам. Отдельно выделена проблема динамической деградации, которая заключается в возможном резком уменьшении множества состояний дискретной динамической системы при поступлении информационного сигнала на ее вход. В работе приведен пример такой системы, а также исследован, аналитически и численно, эффект деградации, который возникает при ее использовании.

Ключевые слова: обратимые динамические системы, динамическая деградация, конечномерное кольцо целых чисел, генераторы псевдослучайных последовательностей.

Кириченко Виктор Викторович. Кандидат физико-математических наук.
Кафедра динамики и прочности машин и сопротивления материалов, Национальный технический университет Украины «Киевский политехнический институт имени Игоря Сикорского», Киев, Украина.
Образование: Донецкий национальный университет, Донецк, Украина, (1999).
Направление научной деятельности: теория гироскопов, системы управления и обработка информации.
Количество публикаций: 53.
E-mail: vkir28@gmail.com

Лесина Евгения Викторовна. Кандидат физико-математических наук. Доцент.
Кафедра автоматики и телекоммуникаций, Донецкий национальный технический университет, Покровск, Украина.
Образование: Донецкий национальный университет, Донецк, Украина, (2001).
Направление научной деятельности: дифференциальные уравнения, системы управления и обработка данных.
Количество публикаций: 51.
E-mail: eugenia.lesina@donntu.edu.ua