CRYPTOGRAPHIC METHOD OF STABILIZING CHAOTIC METHOD OF DISTRIBUTED SYSTEMS

[1] Tatiana Ten, [1] Galina Kogay,
[1]*KSTU "Karaganda State Technical University",*
Kazakhstan, 100027, c. Karaganda, B. World 56

We have developed a cryptographic technique based on stabilization of the chaotic behavior of a dynamical system. The proposed cryptographic technique is based on the fact that for sufficiently general series of chaotic dynamical systems where exist periodic disturbances that lead to stabilization of the cycle. The data is encrypted using stabilized cycles. The disturbances are used as the transmitted signal and the map viewing is the key to decrypt the message. As a result, the advanced cryptographic technique serves as the basis for the development of algorithms for cryptographic transformation of the information based on chaotic mapping.

Keywords: cryptographic technique, chaotic behavior stabilization, encryption.

Introduction

The fact is known from the theory of dynamic system [1-4] that a sufficiently large family of chaotic dynamic systems features periodic disturbances that destabilize the cycle of a given period. The advanced cryptographic technique is based exactly on this fact; the data are encoded with this technique. The transmitted signal uses the disturbances ant the mapping type serves as the key to decoding the received message (in other words, the function setting the mapping).

Technique

The task is to develop the cryptographic technique based on stabilizing the dynamic system chaotic behavior; to explore all the necessary parameters of this cryptographic technique.

Main part

Let us consider the main postulates and the results obtained in the theory of dynamic systems regarding the chaotic behavior stabilization. Presently the most successful techniques of behavior (in other words, the behavior management) of dynamic systems are the technique of multiplicative effect with feedback and the technique without feedback [4, 5]. Let us assume that the system in question is determined with the common differential equations of the following type:

$$\dot{x} = v(x, a), \quad (1.1)$$

where $x = \{x_1, ..., x_n\}$ is the combination of dynamic variables, $v = \{v_1, ..., v_n\}$ is some n-componential function and a is the governing parameter. The problem of controlling the system behavior (1.1) is to find which external disturbance G induces the phase flow $F^t(x,G)$ when the disturbed dynamic system generates it at

$$\dot{x} = v'(x,a,G) \quad (1.2)$$

tends to the selected subset $A(G)$ of its phase space.

The subset $A(G)$ can be booth the attractor and the unstable set. In the latter case, the disturbances G modify the system (1.1) in such a way that thee phase trajectories approach the subset $A(G)$ ad remain within its rather close vicinity $U \supset A(G)$ under the effect of G .

If the external disturbances are due to their multiplicative effect in respect too the dynamic variables x_i, then they are said that their parametric (or multiplicative) control takes place because, as a rule, the parameters are multiplicatively incorporated into the dynamic system.

In this case, the control implies such modification of the function v in respect to (1.1) that the new system $\dot{x} = v'(x,a',t)$ should have the required (selected in advance) behavior. Here $v'(x,a',t) = v'(x,a_0 + a_1(t))$ and the parameter $a_1(t)$ are usually a T-periodic function.

When the parametric disturbances are with the feedback, the current system state is taken into account: $v'(x,a',t) = v(x,a(x(t)))$. The parameter a should change in a special manner rather than periodically.

The situation is rather frequent in applications when the multiplicative behavior of external disturbance in the system is feasible. Then the phase flow $F^t(x,G)$ is factored into two components: the component corresponding to the non-disturbed phase flow $F^t(x)$, and the component $F^t(G)$ initiated exclusively by disturbances $F^t(x,G) = F^t(x) + F^t(G)$. The additive disturbance occurs in this case, in other words, $v'(x,a',t) = v(x,a) + g(t)$, where $g(t)$ designates the external effect. Therefore, the dynamic system control implies the force component application to the vector function. Hence, this type of dynamic system behavior is termed forceful. In its turn, if the force control takes into account the feedback, then the function v is modified as $v'_i = v_i(x,a) + g_k(x_i(t))$, $i = 1,2, ..., n$, $1 \le k \le n$.

Due to a number of reasons, the parametric dynamic stabilization technique has definite advantages over the force one. First, the applications to chemical physical and other essential systems often take into account the values, which are proportional to dynamic variables x_i. Such

systems have $v(0,a_1,...,a_m) = 0$, while the hypersurfaces x_i are invariant sets. It means that system (1.1) reflects real processes only at the simplex $X = \left\{ x \middle| x_i > 0, \sum_{i=1}^{n} x_i < const \right\}$.

The external additive disturbance, in this vase, can lead to the phase trajectories leaving the set X intersecting the hypersurfaces xj =0. Since the force effect can cause degeneration of the system or its issue to the undesirable evolution mode. For instance, it means the extinction of a part of species in the biological systems. Meanwhile, the parametric effect implies the modification of the system resources, thus, it is finer than the force one. Second, the force disturbance is harder to implement. For instance, the force control of chemical systems implies the introduction (and elimination, respectively) of additional substances; the stabilization technique can be achieved in biological systems can be achieved by sterilizing a part of species or by introducing additional species into the colony. On the other had, in opposition to the parametric stabilization, the force technique, as a rule, leads to the desired result in almost all systems. It is because the natural behavior can be literally suppressed by any external force. The feedback introduction is a certain advantage because this control technique ensures the needed result in most cases: the saddle limit cycle selected beforehand is stabilized, thus, the system in question acquires the required motion mode. But this technique is effective only provided the imaging point is located close to the selected cycle. Otherwise, additional techniques of effect should be weighed. Meanwhile, the stabilization technique without feedback does not require any permanent computer (or any other) tracing of the system condition and it is less vulnerable to noise significantly simplifying its use in applications.

The main results obtained from the theory of dynamic systems and due to the stabilization of chaotic behavior exposed to external disturbances without feedback are the following [5, 6]. Assume the dynamic system (mapping) is specified as $T_a: M \to M$,

$$T_a: x \mapsto f(x,a), \quad (1.3)$$

where $a \in A \subset$ R and $f = \{f_1, \ldots, f_n\}$, x = $\{x_1, \ldots, x_n\}$. assume that this system has a chaotic behavior at definite parameter settings , in other words, there is a certain subset A_c, $A_c \subset A$, that the dynamics at $a \in A_c$ (1.3) (possible at some initial conditions) differ from the stationary, periodic or quasiperiodic dynamics. To stabilizey the chaotic behavior, it is necessary to determine the disturbance G affective at the chaotic subset A_c, $G: A_c \to A_c$,

$$G: a \mapsto g(a), a \in A_c, \quad (1.4)$$

so that the resulting disturbed dynamic system

$$T_a : \begin{cases} x \mapsto f(x,a), \\ a \mapsto g(a), x \in M, a \in A_c, \end{cases} \quad (1.5)$$

possesses stable cycles. During periodic disturbance, the transformation G setting the law of parameter modification is determined by the final set of points $\{a_1, a_2, \ldots, a_\tau\}$, being $a_{i+1} = g(a_i)$, $i = 1,2,\ldots \tau\text{-}1$, and $a_1 = g(a_\tau)$, $a_1, a_2, \ldots, a_\tau \in A_c$. in this case it is convenient to apply to each disturbance of the period τ of parameter the relevant vector $\hat{a} = (a_1,\ldots,a_\tau)$ from the space R^τ.

Then the subset

$$A_c = \{\hat{a} \in A_c \otimes A_c \otimes \ldots \otimes A_c : \hat{a} = (a_1,\ldots,a_\tau), a_i \neq a_j, 1 \le i, j \le \tau, i \neq j, a_1,\ldots,a_\tau \in A_c\}$$

$A_c \subset R^\tau$ can be considered as satisfying possible effects of the period τ, operating with A_c.

works [6, 7] manifest that among the sets $\{\hat{a}\} = \{a_1, a_2, \ldots, a_\tau\}$ making up the set A_c there are such $\{a_1^d, a_2^d, a_\tau^d\} = A_d \subset A_c$ that mapping (1.5) possesses stable cycles of limit periods, the period t of the obtained stable cycle being multiple of the period of disturbance, $t = \tau k$, where $\kappa = 1,2,\ldots$. This situation turns out typical for a large class of chaotic mappings [8-10]. In addition, the disturbances $a_1, a_2, \ldots, a_\tau$ can be found for any family of unimodal and piece-linear mappings which have the disturbed series with stable cycles and assigned periods.

This result is based on the following property: if the mapping $T_a: x \mapsto f(x,a)$, $x \in M$, $a \in A$, has such a subset $\sigma \in M$ that $a^* \in A$ is to be found for any x_1, $x_2 \in \sigma$, for which $f(x_1,a^*) = x_2$ and there is a critical point $x_c \in \sigma$ so that $\partial f(x,a)/\partial x|_{x=x_c} \equiv D_x f(x_c,a) = 0$ at any $a \in A$, then for any x_2, x_3, ..., $x_t \in \sigma$, $t = \tau$, there are such x_1 and $a_1, a_2, \ldots, a_\tau$, that the cycle $(x_1, x_2, \ldots, x_t)$ $t = \tau$, represents the stable cycle of disturbed mapping T_a at parametric disturbances $a_1, a_2, \ldots, a_\tau$.

In the general case, the subset A_d corresponding to the stabilized behavior has a rather intricate structure [9, 10]. However, for the quadratic series

$$T_a: x \mapsto ax(1\text{-}x), \quad (1.6)$$

with the periodic disturbance $(a_1, a_2, \ldots, a_\tau)$ the subset A_d corresponding to the cycles of period $t = \tau$ turns out the whole region and it is fractioned into subregions that the disturbances within each subregion yields the stabilization cycle of a definite period. Exactly this result permits to use effectively this mapping to encode and dispatch the latent messages.

Let's consider in detail the periodically (with the period τ) disturbed series (1.6). it is convenient o rewrite it in the following way:

$$\begin{cases} x_{n+1} = a_n x_n (1 - x_n), \\ a_n = a_{n \bmod \tau + 1} \end{cases} \quad (1.7)$$

If this mapping has the cycle of a period $t = \tau$, $p = (x_1, x_2, ..., x_t)$, then the points of this cycle satisfy the following system of equations

$$\begin{cases} x_2 = a_1 x_1 (1 - x_1), \\ x_3 = a_2 x_2 (1 - x_2), \\ \quad ....., \\ x_1 = a_t x_t (1 - x_t). \end{cases} \quad (1.8)$$

To solve the inverse problem, in other words, to find the parameters at which the mapping (1.7) possesses a given cycle $p = (x_1, x_2, ..., x_t)$, it is necessary to express a_i from the system (1.8):

$$a_1 = \frac{x_2}{x_1(1 - x_1)}, \quad a_2 = \frac{x_3}{x_2(1 - x_2)}, \quad a_t = \frac{x_1}{x_t(1 - x_t)}. \quad (1.9)$$

It is apparent that not at all $x_t \in (0,1)$ there is $a_i \in [0,4]$. But, providing this condition is satisfied at any cycle $p = (x_1, x_2, ..., x_t)$, the parameters will be found $(a_1, a_2, \ldots, a_t)$ at which disturbed mapping (1.7) possesses the cycle p. At $|\beta(p)| \equiv \left| \prod_{i=1}^{t} a_i (1 - 2x_i) \right| < 1$ it is stable.

Taking to account equalities (1.9), this condition is written in the following way:

$$|\beta(p)| = \left| \prod_{i=1}^{t} \frac{x_{i+1}}{x_i(1 - x_i)} (1 - 2x_i) \right| = \left| \prod_{i=1}^{t} \frac{1 - 2x_i}{1 - x_i} \right| < 1. \quad (1.10)$$

Since at $x_c = 1/2$ we have $(1 - 2x_c)/(1 - x_c) = 0$, then inequality (1.10) is always implementable. The series of values $(x_1, x_2, ..., x_t)$, at which $a_i \in [0,4]$, inequality (1.10) is satisfied turning space R^t into the definite region with each point corresponding to the stable cycle of disturbed mapping. The transformation of this region with the system (1.9) yields the relevant region of parameters in the parametric space R^t.

The advanced cryptographic technique based on the stabilization of dynamic system chaotic behavior serves as the starting point for development of algorithms of cryptographic data transformation using the chaotic mapping.

Conclusions

The advanced cryptographic technique is based on the fact known from the theory of dynamic systems: there are periodic disturbances in sufficiently common series of chaotic dynamic systems leading to cycle stabilization within the set period. The data is encoded using these stabilized cycles. The disturbances serve as the transmitted signal with the mapping type serving as the key to decoding the received message.

The software is available at present implementing the cryptographic technique based on the stabilization of chaotic behavior of dynamic systems [11].

References

1. Loskutov, A.Ju., S.D. Rybalko and A.A. Churaev, 2004. System of data encoding using stabilization cycles of dynamic systems. Correspondence to JTF, 30 (20): 1-7.
2. Loskutov, A.Ju., E.O. Petrenko, S.D. Rybalko and A.A. Churaev, 2004. Development of data encoding system implemented on the basis of stabilization cycles of maps of non-linear dynamic systems. Scientific session of MIFI-2004. 2.
3. Proc. Of the SPIE 1993 Annual Meeting «Chaos in Communication». San Diego California, 2038.
4. Dmitriev, A.S., 1991. A. data registration and identification in one-dimensional dynamic systems. Radioengineering and electronics, 5: 101-108.
5. Loskutov, A.Yu. and A.I. Shishmarev, 1994. Control of dynamical systems behavior by parametric disturbances and analytic approach. Chaos, 4 (2): 351-355.
6. Bainsby, M.A. and A.R. Oinarov, 2007. Determined chaos in economic system evolution. Institute of automation of NAN KR, Bishkek, Ilim, pp: 37-40.
7. Ten, T.L., M.A. Bainsby, and G.D. Coguy, 2012. Development of data protection system in distributed nets. Karaganda, KarGTU, pp: 193-197.
8. Alekseev, V.V. and A.Yu. Loskutov, 1987. Management of system with strange attractor using parametric effect. USSR Far East Acad. Scie., 293 (6): 1346-1348.
9. Marino, I.P., L. Lopez and M.A. Sanjuan, 2002. Channel coding in communications using chaos. Physics Letters A., 295, pp: 185-191.
10. Bainsby, M.A., T.L. Ten and G.D. Coguy, 2013. Management of determined chaos in distributed nets. Manual, Karaganda, KarGTU, pp:113-124.