applied sciences

MDPI

Article

A Chaotic Secure Communication System Design Based on Iterative Learning Control Theory

Leonardo Acho

Escola d'Enginyeria de Barcelona Est-EEBE, Universitat Politècnica de Catalunya-UPC, Eduard Maristany, 10-14 08019 Sant Adrià de Besòs, Spain; leonardo.acho@upc.edu; Tel.: +34-934-137-240

Academic Editor: Chien-Hung Liu
Received: 25 August 2016; Accepted: 17 October 2016; Published: 22 October 2016

Abstract: This paper presents an application of Iterative Learning Control (ILC) theory to secure communication system design by using chaotic signals, where the logistic-map is employed as a source of chaos. Meanwhile, the ILC scheme is employed as a tool to encrypt and decrypt a message. A set of numerical experiments is realized to evidence the performance of our system, including the noisy case on the channels of communication of the proposed scheme.

Keywords: chaos secure communication; iterative learning control; logistic-map

1. Introduction

Iterative Learning Control theory (ILC; the staple of ILC can be found in a U.S. patent filled in 1967 and available in 1971 [1]) is basically a control strategy to improve transient response (or similarly, the controller performance) of dynamical systems that operate repetitively (also called *multi-pass* or *repetitive* dynamic processes). This is done by adjusting the system control input(s) during the system cycle operations [1–4]. Because the system executes the same task multiple times, the control law may learn from the previous system action (or iteration). Hence, the central challenger of ILC design is to use this information from the previous operation to learn and improve the controller execution over the next iteration by following a control objective. Basically, a repetitive dynamic system is a process that has the following two properties:

- Repetitive action, and
- Iteration.

The first one is the process action that it is periodically repeated, and the second one is the natural iteration between the plant vector state and the repetitive process action.

On the other hand, ILC control strategy has been widely employed in many industrial applications, including manufacturing, robotics, chemical process, among many others [1]. Furthermore, the main benefits of iterative learning control framework are its low transient tracking error, despite large model uncertainty and disturbances [1,5,6], its short a priori knowledge about the system to be controlled, and its low computational effort for control realization [7].

To note, ILC theory has also been used in system modeling, two-dimensional systems analysis, linear matrix inequality system design, and in adaptive and robust control innovation (see, for instance, [5,6] and references therein). In the meantime, some other ILC strategies are mainly based on Lyapunov's theory [8–10].

Finally, many of the available ILC approaches require identical *resetting initial conditions* (at the beginning of each iteration: the well known *resetting condition*); however, in real applications, the perfect resetting condition may be not realizable [6,8]. Therefore, under different tests on resetting initial conditions, the boundedness along the time evolution and asymptotic stability on each iteration

of an ILC system were well proven in [8]. Actually, this is an important robust property of the ILC tool to design new engineering developments, such as secure communication systems subject to noisy environments.

In this paper, motivated by the *canonical* ILC structure stated in [8], a chaotic secure communication scheme is developed. This design is based on the chaotic logistic-map. Therefore, the proposed design uses the ILC method as a base tool to encrypt and decrypt a message, recalling that the development of new chaotic secure communication systems is still an important open topic [11–15].

The remainder of this paper is organized as follows. In Section 2, the canonical ILC frame is retrieved from [8]. Section 3 presents our ILC chaotic secure communication system design. Performance numerical evaluation of our scheme is evidenced in Section 4. Finally, the conclusions are given in Section 5, including future issues on the subject.

2. The Canonical ILC System

Let us consider the next first-order nonlinear system in the i-th iteration [8]:

$$\dot{x}_i = \theta(t)\xi(x_i, t) + u_i, \quad t \in [0, T], \quad x(0) = x_0, \tag{1}$$

where $\xi(x_i, t)(= \xi_i$ for simplicity) is a known nonlinear function which can be locally Lipschitz, $\theta(t) \in C[0, T]$ is the *unknown* time-varying parameter, and T represents the iteration (or operation) time.

Given the reference trajectory supplied by:

$$\dot{x}_r = f(x_r, r, t), \tag{2}$$

where $f_r = f(x_r, r, t)$ is a known smooth-function and r is a reference input signal which produces a bounded response $x_r(t)$ over the time interval $[0, T]$, the *ILC objective* is to find a sequence of appropriate control inputs u_i for $t \in [0, T]$ such that the system state x_i tracks (as well as possible) the reference trajectory x_r as $i \to \infty$ [8].

A solution to the ILC objective is as follows [8]:

$$u_i = ke_i + f_r - \hat{\theta}_i(t)\xi_i, \tag{3}$$

$$\hat{\theta}_i(t) = \text{proj}(\hat{\theta}_{i-1}(t)) - \xi_i e_i, \quad \hat{\theta}_{-1}(t) = 0, \tag{4}$$

where $e_i = e_i(t) = x_r(t) - x_i(t)$,

$$\text{proj}(x) = \begin{cases} x, & \mid x \mid \leq \theta^* \\ \text{sign}(x)\theta^*, & \text{otherwise} \end{cases}; \tag{5}$$

and θ^* is the *parameter projection bound*, assumed sufficiently large. According to [8], this ILC—even under random and bounded initial conditions $e_i(0)$ (if $e_i(0) = 0$ implies *ideal* resetting condition.)—assures the ILC control objective. Finally, the *learning* parameter $\hat{\theta}_i(t)$ gives an estimation of the time-varying parameter $\theta(t)$ over each iteration of the repetitive process.

3. Chaotic Secure Communication Design Based on ILC Theory

This section presents our secure communication system design by employing the chaotic *logistic-map* and by using the ILC framework as a tool to encrypt and decrypt a message. We are going to use its property for the estimation of the unknown time-varying parameter $\theta(t)$.

To begin with, let us refer to the main block diagram shown in Figure 1. Allow us to define the *transmitter* block as:

$$\dot{x}_i = \theta(t)\xi_i + u_i, \quad x_i(0) = x_{i-1}(T). \tag{6}$$

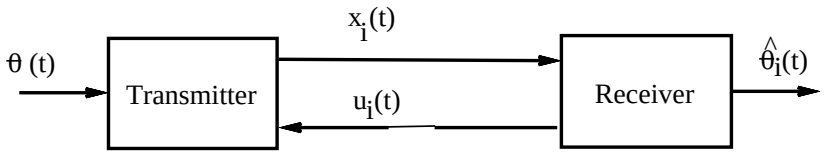

Figure 1. Block diagram of the proposed secure communication system.

The initial conditions $x_i(0) = x_{i-1}(T)$ means that the end state of the preceding iteration becomes the initial state for the new one. Here, $\theta(t)$ represents the message to be encrypted. In our design, we are using a two-channel communication system. The transmitted signal $x_i(t)$ goes on one channel, and on the other travels the generated signal $u_i(t)$ coming from the receiver (see Figure 1). Both signals have to be in *random-like* behavior with the message encrypted in $x_i(t)$. Then, $\hat{\theta}_i(t)$ becomes the decrypted signal (an estimation of the transmitted message in $\theta(t)$). To complete our design for the transmitter section, let us define $\xi_i = x_i(1 - x_i)$, a *mimic* expression from the chaotic logistic-map.

Now, *designing* the *receiver* block as:

$$\begin{aligned} \dot{x}_r &= -x_r + z(j), \quad x_r(0) = 0.1, && (7)\\ \hat{\theta}_i(t) &= \text{proj}(\hat{\theta}_{i-1}(t)) - \xi_i e_i, \quad \hat{\theta}_{-1} = 0, && (8)\\ e_i(t) &= x_r(t) - x_i(t), && (9)\\ u_i(t) &= k e_i(t) + f_r - \hat{\theta}_i(t)\xi_i, && (10) \end{aligned}$$

where $z(j)$ is realized by employing the well-known discrete-time *chaotic* logistic-system:

$$z(j+1) = 4z(j)(1 - z(j)), \quad z(0) = 0.1 \text{ (we set } z(0) = x_r(0), \text{ but it does not matter)}, \quad j = 0, 1, 2, 3, \cdots . \tag{11}$$

The output of the logistic-map $z(j)$ (utilized as the reference signal $r = r(t)$ to f_r) is assumed being performed having a *zero-order-holder* device (ZOH), T being the time duration between discrete-time samples. Recall that the *ZOH* device is a transformation mechanism to translate a *discrete-time* signal to a piece-wise *continuous-time* one (see, for instance, Chapter 1 in [16]).

Stability issue—The stability issue of the overall closed-loop communication system is warranted by the results given in [9] and stated in Section 2, including its robustness property.

4. Numerical Experiments

To display numerical experiment results, let us complete our secure communication design by using $T = 1$ s, $\theta^* = 10$ Rad, and $k = 10$, and again, $\xi_i = x_i(1 - x_i)$. The test message used as $\theta(t)$ and the obtained estimation of the message $\hat{\theta}_i(t)$ at the receiver part are shown in Figure 2. Figure 3 shows $x_r(t)$ and $x_i(t)$. We can appreciate a random-like behavior on these, due to the chaotic logistic-map employed in our system. Because they are too similar, Figure 4 displays a zoomed-in version of the error dynamic. The signal $u_i(t)$ is pictured in Figure 5. Finally, Figure 6 illustrates the numerical results when random noises are presented on each channel of the communication system, where we insert uncorrelated normal distribution noises with zero mean and standard deviation of 0.05. For comparison, Figure 7 displays the error dynamic for the noisy case. From this, we can note that the external noise helps, in some way, to better hide our secret message.

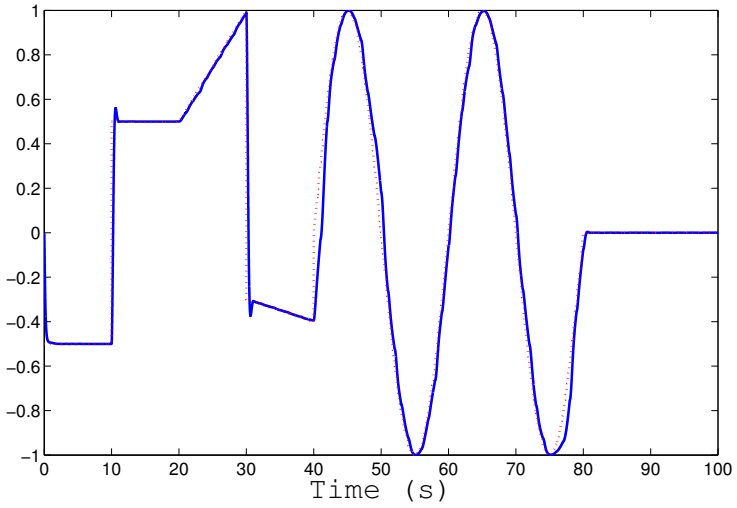

Figure 2. Numerical results: red-dotted line is $\theta(t)$ and the other one is $\hat{\theta}(t)$.

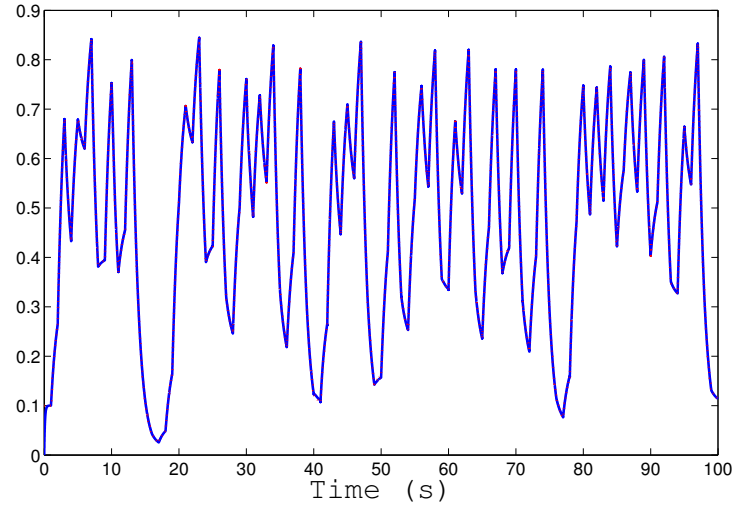

Figure 3. Numerical results: red-dotted line is $x_r(t)$ and the other one is $x_i(t)$.

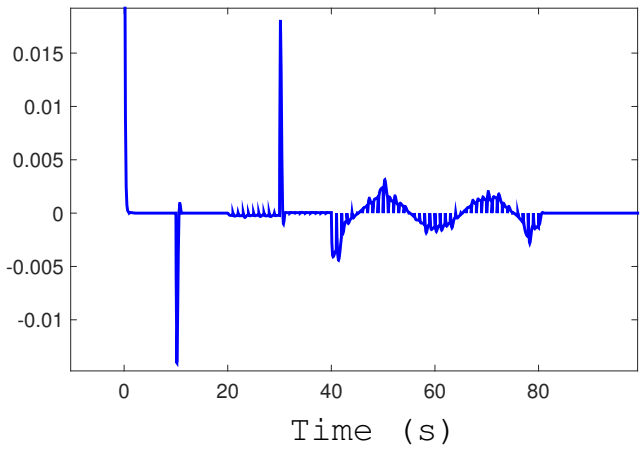

Figure 4. Numerical results: $e_i(t)$.

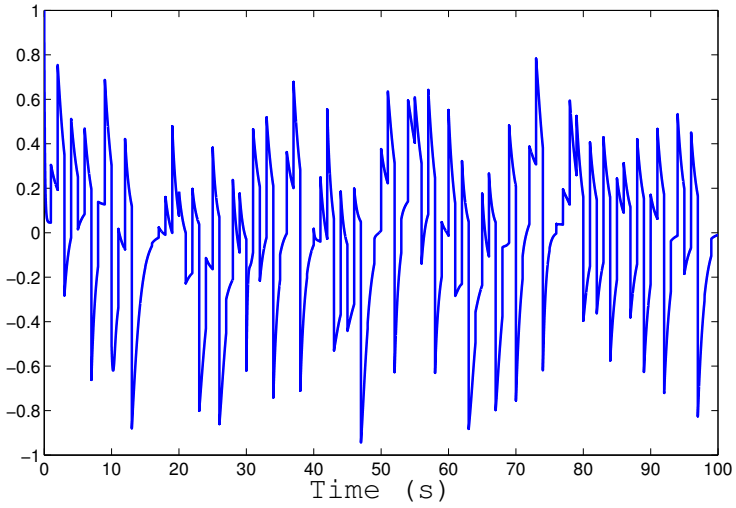

Figure 5. Numerical results: $u_i(t)$.

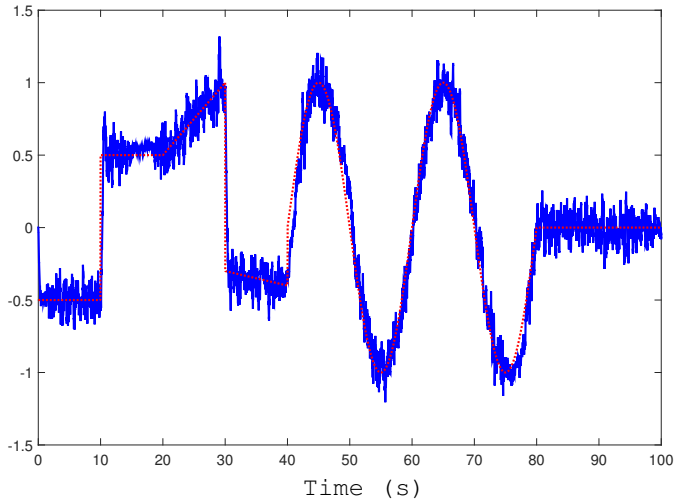

Figure 6. Numerical results for the noisy case: red-dotted line is $\theta(t)$ and the other one is $\hat{\theta}(t)$.

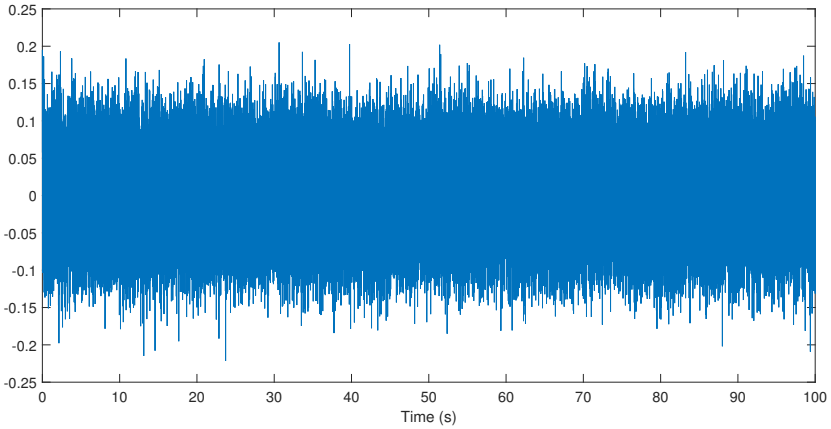

Figure 7. Numerical results for the noisy case: $e_i(t)$.

5. Conclusions

This paper has described an application of the ILC theory to secure communication system design by using a chaotic signal obtained from the chaotic-logistic map. It was also evidenced that the main important benefit of the proposed ILC given in [8] is robustness, even on variation in the resetting initial conditions and exogenous noise. From our secure communication system, an important design parameter is the T-time duration of each cycle. By reducing it, we may be able to employ our system to more "faster-time" message signals. It is worth mentioning that the ILC method belongs to the *data-driven* systems, due to data measurement used in its learning algorithm [17].

Finally, we believe that it is important to highlight that the main aim of this paper is to illustrate a kind of academic example of an application of the ILC theory to secure communication system design based on chaotic signals. However, and because it is beyond the author's expertise, an additional analysis test is missing; for instance, the bit error rate curve over AWGN (Additive White Gaussian Noise) channel, including the possibility to expand our design by using the latest works on chaotic waveform to convey data such as DCSK (Differential Chaos Shift Keying), NR-DCSK (Noise Reduction Differential Chaos Shift Keying), and so on. All of these are left for a future work.

Acknowledgments: Research supported in part by the Spanish Ministry of Economy and Competitiveness through the research grant project DPI2015-64170-R/FEDER.

Conflicts of Interest: The author declares no conflict of interest.

Abbreviations

The following abbreviation is used in this manuscript:

ILC	Iterative Leaning Control
ZOH	Zero-Order-Holder

References

1. Bristow, D.A.; Tharayil, M.; Alleyne, A.G. A survey of iterative learning control. *IEEE Control Syst.* **2006**, *26*, 96–114.
2. Ahn, H.S.; Chen, Y.; Moore, K.L. Iterative learning control: Brief survey and categorization. *IEEE Tran. Syst. Man Cybern. C Appl. Rev.* **2007**, *37*, 1099.
3. Chen, W.; Chen, Y.Q.; Yeh, C.P. Robust iterative learning control via continuous sliding-mode technique with validation on an SRV02 rotary plant. *Mechatronics* **2012**, *22*, 588–593.
4. Zhang, C.L.; Li, J.M. Adaptive iterative learning control of non-uniform trajectory tracking for strict feedback nonlinear time-varying systems. *Int. J. Autom. Comput.* **2014**, *11*, 621–626.
5. Madady, A. An extended PID type iterative learning control. *Int. J. Control Autom. Syst.* **2013**, *11*, 470–481.
6. Bouakrif, F.; Boukhetala, D.; Boudjema, F. Velocity observer-based iterative learning control for robot manipulators. *Int. J. Syst. Sci.* **2013**, *44*, 214–222.
7. Chen, Y.; Wen, C. *Iterative Learning Control: Convergence, Robustness and Applications*; Springer: Heidelberg, Germany, 1999.
8. Xu, J.X.; Yan, R.; Chen, Y.Q. On initial conditions in iterative learning control. *IEEE Trans. Autom. Control* **2005**, *50*, 1349–1354.
9. Xu, J.X.; Tan, Y. *Linear and Nonlinear Iterative Learning Control*; Springer: Heidelberg, Germany, 2003; Volume 291.
10. Tayebi, A. Adaptive iterative learning control for robot manipulators. *Automatica* **2004**, *40*, 1195–1203.
11. Zapateiro, M.; Vidal, Y.; Acho, L. A secure communication scheme based on chaotic Duffing oscillators and frequency estimation for the transmission of binary-coded messages. *Commun. Nonlinear Sci. Numer. Simul.* **2014**, *19*, 991–1003.
12. Yang, J.; Chen, Y.; Zhu, F. Associated observer-based synchronization for uncertain chaotic systems subject to channel noise and chaos-based secure communication. *Neurocomputing* **2015**, *167*, 587–595.

13. Zapateiro De la Hoz, M.; Acho, L.; Vidal, Y. An Experimental Realization of a Chaos-Based Secure Communication Using Arduino Microcontrollers. *Sci. World J.* **2015**, *2015*, 123080.
14. Acho, L. A discrete-time chaotic oscillator based on the logistic map: A secure communication scheme and a simple experiment using Arduino. *J. Frankl. Inst.* **2015**, *352*, 3113–3121.
15. Yang, T. A survey of chaotic secure communication systems. *Int. J. Comput. Cognit.* **2004**, *2*, 81–130.
16. Ogata, K. *Discrete-Time Control Systems*; Prentice Hall: Englewood Cliffs, NJ, USA, 1995; Volume 2.
17. Xu, D.; Jiang, B.; Shi, P. Adaptive observer based data-driven control for nonlinear discrete-time processes. *IEEE Trans. Autom. Sci. Eng.* **2014**, *11*, 1037–1045.