International Journal of Automation and Computing

12(3), June 2015, 297-306
DOI: 10.1007/s11633-015-0887-9

Nonlinear Masking and Iterative Learning Decryption for Secure Communications

Ming-Xuan Sun

College of Information Engineering, Zhejiang University of Technology, Hangzhou 310023, China

Abstract: Typical masking techniques adopted in the conventional secure communication schemes are the additive masking and modulation by multiplication. In order to enhance security, this paper presents a nonlinear masking methodology, applicable to the conventional schemes. In the proposed cryptographic scheme, the plaintext spans over a pre-specified finite-time interval, which is modulated through parameter modulation, and masked chaotically by a nonlinear mechanism. An efficient iterative learning algorithm is exploited for decryption, and the sufficient condition for convergence is derived, by which the learning gain can be chosen. Case studies are conducted to demonstrate the effectiveness of the proposed masking method.

Keywords: Secure communication, masking, convergence, learning algorithms, nonlinearities.

1 Introduction

Chaotic behavior has been observed in a variety of dynamical systems, and received intensive researches both theoretically and experimentally. A chaotic system is nonlinear, which exhibits sensitive, unpredictable and random-seeming behavior. Nevertheless, its state variables are bounded, and change with time in a deterministic manner. Chaos is considered to be a desirable phenomenon for use in potential applications to various fields, especially in secure communication. Investigation on application of chaos to cryptography was initiated by the work of synchronizing drive-response chaotic systems in [1], which has witnessed a rapid development in the recent years[2−4].

There are efficient schemes proposed for encrypting plaintext data for transmission through open channels. Typical additive chaotic masking generates the transmitted signal, by adding the chaotic signal to the plaintext at the transmitter as

$$s(t) = x(t) + p(t) \tag{1}$$

where x is the chaotic mask, p is the plaintext, and s is the information bearing signal to be transmitted. As s is obtained and the synchronization occurs on the receiver side, the plaintext p can be recovered by subtracting the synchronized signal from s. Chaotic modulation by multiplication is another useful masking method, described by

$$s(t) = x(t)p(t). \tag{2}$$

When the synchronization occurs on the receiver side, the plaintext p can be reconstructed by dividing the synchronized signal from s. Precautions have to be made for avoiding the possible singularity problem as the synchronized signal for $x(t)$ may achieve zero at some time instants. Related modulation schemes are the chaotic parameter modulation[5, 6], which uses the signal to be encrypted to change the parameter of the chaotic transmitter.

In the aforementioned typical schemes, the inversion computing for decrypting is simple as they are linear in their arguments. The linearity nature leads to easy implementations of these schemes, but also allows ease of breaking. In the published literature, there exist efforts made for enhancing security. One way is to increase nonlinearity of the masking mechanism to be applied[7−8]. It is observed that higher nonlinearity may lead to higher security. The major difficulty, however, lies in the inversion computing for decrypting.

Instead of the drive-response viewpoint, the concept of synchronization was further explored in [9] to link the classical notion of observers from control theory. This motivated attempts to apply such an observer-based synchronization methodology to chaotic communication. As a synchronization system is not available, parameter identification methods are alternative for chaotic communication[10], where parameter modulation is applied. Identification algorithms, with nice performance for tracking time-varying parameters, can be used to demodulate the signal of transmission.

In this paper, we shall formulate the problem of secure communication in terms of iterative learning[11−14]. An initial effort can be found in [15]. The learning algorithm is efficient for estimating time-varying parameters spanned over a finite time interval in a dynamical system. Nonlinear masking is adopted in our schemes and the difficulty in the inversion computing is avoided. The plaintext is assumed

Regular Paper
Special Issue on Latest Advances in ILC/RLC Theory and Applications
Manuscript received April 29, 2014; accepted October 28, 2014
Recommended by Guest Editor Rong-Hu Chi
This work was supported by National Natural Science Foundation of China (No. 61174034).

to be given over a pre-specified time interval. The learning algorithm uses only the transmitted signal s. Through learning, the plaintext can be recovered from the ciphertext. On the other hand, no synchronization occurs. The iterative learning method is related with the inversion system based approach[16−18]. However, our proposed learning algorithm is simple and does not need inversion computing. By comparing the proposed learning algorithm with the existing ones, it can been seen that 1) the unknowns to be estimated are not assumed to be slowly time varying, and 2) the learning algorithm ensures the consistency of estimates. In addition, a checkable convergence condition is given for the learning gain selection. The organization of the paper is as follows. For dealing with nonlinear masking, in Section 2, chaotic secure communication is formulated in terms of time-varying parameter identification problems, and the iterative learning methodology is shown to be applicable to solving such problems. Performance analysis for the proposed learning algorithm is given in Section 3. Two fundamental techniques are suggested for enhancing security of the iterative learning based communication in Section 4. Numerical results are presented in Section 5, and Section 6 draws the conclusions.

2 A secure communication system

Iterative learning offers an efficient tool for estimating time-varying unknowns in a dynamical system over a finite interval. The problem of chaotic secure communication is formulated based on this methodology of learning in this section.

2.1 Nonlinear masking

In our cryptographic scheme, the transmitter adopts a chaotic system of the form

$$\dot{x} = f(x, \alpha) \tag{3}$$

where $x \in \mathbf{R}^n$ is the state vector of the system, and α is the parameter chosen for the masking purpose, satisfying that $\alpha_{\min} \leq \alpha \leq \alpha_{\max}$. The system could exhibit chaotic behavior as the parameter α varies within the region. A typical chaotic system is given in [19]. The nonlinear function f is assumed to be smooth on $\mathbf{R}^n$.

Let $p(t)$ denote the plaintext to be transmitted, which is assumed to satisfy that $\alpha_{\min} \leq p(t) \leq \alpha_{\max}$. Here, we simply replace α with $p(t)$ in (3) to obtain

$$\dot{x} = f(x, p). \tag{4}$$

The transmitted signal is constructed in the way of

$$s = g(x, p) \tag{5}$$

where x is the state given by (4). The nonlinear function g is chosen by designer such that s is bounded. The design of function g is an important procedure to enhance the degree of security. This will be clarified further in Section 4 and is justified in Section 5.

2.2 Iterative learning decryption

The duration of the plaintext $p(t)$ is assumed to be finite, i.e., $t \in [0, T]$ and $T > 0$ is finite. Given a tolerance error bound ϵ, the recovery objective on the receiver side is to find text $p_k(t), t \in [0, T]$ and $k = 0, 1, 2, \cdots$, where k indicates the iteration index, so that as iteration increases, the error between $p_k(t)$ and $p(t)$ will be within the tolerance error bound, i.e., $|p(t) - p_k(t)| \leq \epsilon$, $t \in [0, T]$. In this paper, we shall develop a learning algorithm to generate the texts $p_k(t)$, $t \in [0, T]$. $p(t)$ can be recovered from the ciphertext via learning. Throughout this paper, let us denote by $|a|$ the absolution value for a scalar a, and $|a| = \max_{1 \leq i \leq n} |a_i|$ for an n-dimensional vector $a = [a_1, \cdots, a_n]^{\mathrm{T}}$. The λ-norm for a time function $b(t)$ is defined as $|b|_\lambda = \sup_{t \in [0,T]} \{\mathrm{e}^{-\lambda t} |b(t)|\}, \lambda > 0$.

The learning procedure is presented as follows:

Given the transmitted signal $s(t)$, $t \in [0, T]$, the initial estimate $p_0(t)$, $t \in [0, T]$, the initial condition x_0 and the tolerance error ε:

1) Set $k = 0$ and $p_k(t) = p_0(t)$, $t \in [0, T]$.

2) Put $x_k(0) = x_0$.

3) Obtain $s_k(t)$, $t \in [0, T]$, by solving the following differential equations:

$$\dot{x}_k = f(x_k, p_k) \tag{6}$$

$$s_k = g(x_k, p_k). \tag{7}$$

4) Calculate the error signal $s(t) - s_k(t)$, $t \in [0, T]$.

5) Stop the procedure if $|s(t) - s_k(t)| \leq \varepsilon$, $t \in [0, T]$, otherwise go to 6).

6) Produce $p_{k+1}(t)$, $t \in [0, T]$, by using the update law

$$p_k = \mathrm{sat}(p_{k-1}) + \gamma(s - s_k) \tag{8}$$

with learning gain γ to be designed.

7) Increase k by 1, $k \Leftarrow k + 1$, and goto 2) to repeat the procedure.

In (8), sat is the saturation function defined as, for a scalar b,

$$\mathrm{sat}(b) = \begin{cases} \bar{b}^1, & \text{if } b < \bar{b}^1 \\ b, & \text{if } \bar{b}^1 \leq b \leq \bar{b}^2 \\ \bar{b}^2, & \text{if } b > \bar{b}^2 \end{cases} \tag{9}$$

where $\bar{b} = \{\bar{b}^1, \bar{b}^2\}$ represents the lower and upper bounds, satisfying that $\bar{b}^1 < \bar{b}^2$. Case $\bar{b}^1 \neq -\bar{b}^2$ indicates the asymmetric case. The saturation bounds are chosen appropriately such that the message signal p lies within them. The use of the saturation function aims to ensure the boundedness of p_k.

As for (8), the closed-loop learning is suggested for exploiting the advantage of feedback. However, this method has the defect that the intrinsic time delay exists when obtaining s_k, which would cause performance degradation due to the error between the actual signal and the estimated one. It will be shown that performance improvement can be made theoretically, provided that the estimation error is sufficiently small.

We emphasize the flexibility of choice for learning algorithms, and that the learning law (8) is by no means exclusive. Open-loop learning, using only the data from last cycle instead of the current cycle, can be applicable when one wants the message to be recovered off-line. A fully-saturated learning law is given as

$$p_{k+1}(t) = \mathrm{sat}\big(p^*_{k+1}(t)\big) \tag{10}$$

$$p^*_{k+1}(t) = \mathrm{sat}\big(p^*_k(t)\big) + \gamma\big(s(t) - s_k(t)\big). \tag{11}$$

3 Performance analysis

Without any loss of generality, the state variables of the chaotic system undertaken are assumed to be bounded and there exists subset $X \subset \mathbf{R}^n$ such that $x_k(t) \in X$ for all $t \in [0, T]$ and for all k. As the learning law that we apply is partially saturated, the boundedness of $p_k(t)$ is ensured as well. In order word, there exists subset $P \subset \mathbf{R}$ such that $p_k(t) \in P$ for all $t \in [0, T]$ and for all k.

In practice, the signal s is acquired with the presence of measurement noise. In order to examine the effect of measurement noise, as well as the intrinsic time delay in obtaining s_k, we consider the learning law in the form of

$$p_k = \mathrm{sat}(p_{k-1}) + \gamma(s - s_k) + \eta_k \tag{12}$$

where η_k indicates a variable related to measurement noise as in obtaining s, and the estimation error for s_k. In addition, we rewrite the learning law (10) and (11) to be

$$p_{k+1}(t) = \mathrm{sat}\big(p^*_{k+1}(t)\big) \tag{13}$$

$$p^*_{k+1}(t) = \mathrm{sat}\big(p^*_k(t)\big) + \gamma\big(s(t) - s_k(t)\big) + \eta_k. \tag{14}$$

The initial condition is usually used as a security key in the conventional chaotic secure communication systems. It is expected that any initial condition error will result in failing to decrypt the confidential information. We shall also examine the effect of the initial condition error on performance of the proposed method.

To make the problem more feasible, the following assumptions are imposed.

Assumption 1. $x_k(0)$ is set to $x_0+\epsilon_0$ at the beginning of each cycle, where ϵ_0 is the initial condition error satisfying

$$|x_0 - x_k(0)| = \epsilon_0.$$

Assumption 2. η_k is assumed to satisfy

$$|\eta_k| \le \epsilon_\eta$$

where $\epsilon_\eta > 0$.

Assumption 3. $g_p(x,p) (= \frac{\partial g(x,p)}{\partial p}) \neq 0$ for all $x \in X$ and for all $p \in P$.

Assumption 4. $f(x,p)$ is local Lipschitz in both x and p, i.e., there exists $l_f > 0$ such that

$$|f(x',p') - f(x'',p'')| \le l_f(|x' - x''| + |p' - p''|)$$

for any $x', x'' \in X$ and for any $p', p'' \in P$.

Assumption 5. $g(x,p)$ is local Lipschitz in both x and p, i.e., there exists $l_g > 0$ such that

$$|g(x',p') - g(x'',p'')| \le l_g(|x' - x''| + |p' - p''|)$$

for any $x', x'' \in X$ and for any $p', p'' \in P$.

Under Assumption 1, the initial condition of the receiver is set to $x_0 + \epsilon_0$, while the initial condition of the transmitter is set to x_0. The convergence result of the iterative learning based secure communication system is stated in the following theorem.

With the aid of the following lemma (see Appendix A for the proof), we can establish the convergence of the partially-saturated learning algorithm.

Lemma 1. For real numbers a and b, if $\bar{b}^1 < a < \bar{b}^2$, then

$$|a - \mathrm{sat}(b)|^r \le |a - b|^r \tag{15}$$

where $r > 0$ is a given real number.

Theorem 1. Consider the system consisting of the transmitters (4) and (5), and the receivers (6) and (7), satisfying Assumptions 1−5. Let the learning law (12) be applied with the learning gain chosen to satisfy, for all $x_k \in X$ and for all $\bar{p}_k \in P$,

$$\left|\frac{1}{1 + \gamma g_p(x_k, \bar{p}_k)}\right| \le \rho < 1. \tag{16}$$

Then,

$$\lim_{k\to\infty} \sup |p - p_k|_\lambda \le \frac{\bar{\epsilon}}{1 - \bar{\rho}}$$

with $\bar{\epsilon}, \bar{\rho}$ and $\bar{p}_k$ are to be specified.

Proof. See Appendix B. □

The robustness property of the learning algorithm, given in Theorem 1, is particularly desirable due to its iterative nature. This property ensures the boundedness of the error $p - p_k$, and the achieved error bound depends on the bounds of measurement noise and initial condition error. The robustness result fully characterizes the effect of measurement noise and initial condition error, implying that the recovery of the message will not be easy if the signal to noise ratio is not designed appropriately, or the initial condition is not known exactly.

The convergence result in the absence of uncertainties is presented in Corollary 1.

Corollary 1. Let the system, consisting of the transmitters (4) and (5), and the receivers (6) and (7), satisfy Assumptions 1−5. The learning law (12) is applied with the learning gain chosen to satisfy (16). Then, the error $p(t) - p_k(t)$ converges to zero on $[0, T]$ uniformly as $k \to \infty$, when $\epsilon_0 = 0$ and $\epsilon_\eta = 0$.

Proof. The proof is straightforward by that for Theorem 1. □

By Corollary 1, the zero-error convergence over the entire interval can be guaranteed in the absence of the uncertainties. This implies that exact decryption over the entire interval $[0, T]$ is achieved. We would like to note that the proposed method yields such complete recovery of message, whereas the message recovery by most existing methods is in an asymptotic manner. The complete recovery through learning is useful to enhance the security by designating the starting time of the message in the transmitted signal.

For the open-loop learning, we have the following robustness and convergence results.

Theorem 2. Consider the system consisting of the transmitters (4) and (5), and the receivers (6) and (7), satisfying Assumptions 1−5. Let the learning laws (13) and (14) be applied with the learning gain chosen to satisfy, for all $x_k \in X$ and for all $\bar{p}_k \in P$,

$$|1 - \gamma g_p(x_k, \bar{p}_k)| \leq \rho < 1. \tag{17}$$

Then,

$$\limsup_{k\to\infty} |p - p_k|_\lambda \leq \frac{\bar{\epsilon}}{1-\bar{\rho}}$$

with $\bar{\epsilon}, \bar{\rho}$ and $\bar{p}_k$ are to be specified.

Proof. See Appendix C. □

4 Security enhancements

Two fundamental techniques, in this section, are suggested for enhancing security of the iterative learning based communication scheme presented in Section 2. Here, the results are presented for the closed-loop learning. However, the proposed techniques are also applicable when the open-loop learning algorithm is used.

The first one also generates the signal s in the manner specified by (5). However, instead of the directly replacing α with $p(t)$ in the chaotic system, the transmitted signal is taken to replace the parameter as

$$\dot{x} = f(x, s). \tag{18}$$

The system is assumed to be of chaotic behavior within the region S to which s belongs. On the side of receiver, $s_k(t), t \in [0, T]$, is obtained by solving the differential equations as

$$\dot{x}_k = f(x_k, s_k). \tag{19}$$

Assumption 4′. $f(x, s)$ is local Lipschitz in both x and s, i.e., there exists $l_f > 0$ such that

$$|f(x', s') - f(x'', s'')| \leq l_f(|x' - x''| + |s' - s''|)$$

for all $x \in X$ and for all $s \in S$.

Theorem 3. Consider the system consisting of the transmitters (5) and (18), and the receivers (7) and (19), satisfying Assumptions 1−3, 4′ and 5. Let the update law (12) be applied with the learning gain chosen to satisfy (16). Then, the same results as in Theorem 1 are obtained.

Proof. Integrating both sides of (18) and (19) gives rise to

$$x(t) - x_k(t) \leq x(0) - x_k(0) + \int_0^t \big(f(x, s) - f(x_k, s_k)\big)\mathrm{d}\tau.$$

By Assumptions 1, 4′ and 5, we have

$$\begin{aligned}
&|x(t) - x_k(t)| \leq \\
&\quad |x(0) - x_k(0)| + \int_0^t l_f(|x - x_k| + |s - s_k|)\mathrm{d}\tau \leq \\
&\quad |x(0) - x_k(0)| + \int_0^t l_f\big(|x - x_k| + l_g(|x - x_k| + \\
&\quad |p - p_k|)\big)\mathrm{d}\tau = \\
&\quad \epsilon_0 + \int_0^t l_f((1 + l_g)|x - x_k| + l_g|p - p_k|)\mathrm{d}\tau.
\end{aligned}$$

Using Bellman-Gronwall Lemma yields

$$\begin{aligned}
&|x(t) - x_k(t)| \leq \\
&\quad \epsilon_0 \mathrm{e}^{l_f(1+l_g)t} + l_f l_g \int_0^t \mathrm{e}^{l_f(1+l_g)(t-\tau)}|p - p_k|\mathrm{d}\tau.
\end{aligned} \tag{20}$$

Using the same derivations to arrive at (B3) in Appendix, we obtain

$$|p - p_k| \leq \rho(|p - p_{k-1}| + l_g|\gamma||x - x_k| + \epsilon_\eta). \tag{21}$$

Substituting (20) into (21) results in

$$\begin{aligned}
&|p - p_k| - \rho l_f l_g^2 |\gamma| \int_0^t \mathrm{e}^{l_f(1+l_g)(t-\tau)}|p - p_k|\mathrm{d}\tau \leq \\
&\quad \rho(|p - p_{k-1}| + l_g|\gamma|\epsilon_0 \mathrm{e}^{l_f(1+l_g)t} + \epsilon_\eta).
\end{aligned}$$

As $\lambda > l_f(1 + l_g)$, we have

$$\begin{aligned}
&\left(1 - \rho l_f l_g^2 |\gamma| \frac{1 - \mathrm{e}^{(l_f(1+l_g)-\lambda)T}}{\lambda - l_f(1 + l_g)}\right)|p - p_k|_\lambda \leq \\
&\quad \rho(|p - p_{k-1}|_\lambda + l_g|\gamma|\epsilon_0 + \epsilon_\eta).
\end{aligned} \tag{22}$$

Let us define

$$\begin{aligned}
\bar{\rho} &= \frac{\rho}{1 - \rho l_f l_g^2 |\gamma| \dfrac{1 - \mathrm{e}^{(l_f(1+l_g)-\lambda)T}}{\lambda - l_f(1 + l_g)}} \\
\bar{\epsilon} &= \bar{\rho}(l_g|\gamma|\epsilon_0 + \epsilon_\eta).
\end{aligned}$$

Equation (22) becomes

$$|p - p_k|_\lambda \leq \bar{\rho}|p - p_{k-1}|_\lambda + \bar{\epsilon}.$$

Since $0 \leq \rho < 1$, it is possible to choose a sufficiently large $\lambda (> l_f)$ such that

$$1 - \rho l_f l_g^2 |\gamma| \frac{1 - \mathrm{e}^{(l_f(1+l_g)-\lambda)T}}{\lambda - l_f(1 + l_g)} > 0$$

and $0 \leq \bar{\rho} < 1$. Therefore, we obtain a contraction mapping in $|p - p_k|_\lambda$ and the error will reduce to the bound $\frac{\bar{\epsilon}}{1-\bar{\rho}}$ in the limit. □

One more masking technique is to enhance nonlinearity of the mechanism for generating the signal s, for which we shall use a composite function, formed by the composition of one function on another, i.e.,

$$\begin{aligned}
s &= g(x, s^1) \\
s^1 &= h(x, p).
\end{aligned} \tag{23}$$

On the side of receiver, we use the following for encrypting

$$\begin{aligned} s_k &= g(x_k, s_k^1) \\ s_k^1 &= h(x_k, p_k). \end{aligned} \tag{24}$$

The chaotic system for the masking scheme is the same as (4).

Assumption 5′. $g(x, s)$ is local Lipschitz in both x and s, i.e., there exists $l_g > 0$ such that

$$|g(x', s') - g(x'', s'')| \leq l_g(|x' - x''| + |s' - s''|)$$

for all $x \in X$ and for all $s \in S$.

Assumption 6. $h(x, p)$ is local Lipschitz in both x and p, i.e., there exists $l_h > 0$ such that

$$|h(x', p') - h(x'', p'')| \leq l_h(|x' - x''| + |p' - p''|)$$

for all $x \in X$ and for all $p \in P$.

It follows from the update law (12) that

$$\begin{aligned} &p - p_k = p - \mathrm{sat}(p_{k-1}) - \\ &\quad \gamma\big[g\big(x, h(x,p)\big) - g\big(x_k, h(x_k, p_k)\big)\big] - \eta_k. \end{aligned}$$

By resorting the mean value theorem, $g(x_k, h(x_k, p)) - g(x_k, h(x_k,\ p_k)) = g_h h_p(x_k, \bar{p}_k)(p - p_k)$, $\bar{p}_k = p + (1 - \xi)(p_k - p)$, $0 < \xi < 1$, we obtain

$$\begin{aligned} &\big(1 + \gamma g_h h_p(x_k, \bar{p}_k)\big)(p - p_k) = \\ &\quad p - \mathrm{sat}(p_{k-1}) - \gamma\big[g\big(x, h(x,p)\big) - g\big(x_k, h(x_k, p)\big)\big] - \eta_k. \end{aligned}$$

Taking absolute values on both sides of the above equation, we have

$$\begin{aligned} &|p - p_k| \leq \\ &\quad |1 + \gamma g_h h_p(x_k, \bar{p}_k)]^{-1}|\big[|p - \mathrm{sat}(p_{k-1})| + \\ &\quad |\gamma||g\big(x, h(x,p)\big) - g\big(x_k, h(x_k,p)\big)| + |\eta_k|\big]. \end{aligned}$$

Let γ be chosen such that

$$\left|\frac{1}{1 + \gamma g_h h_p(x_k, \bar{p}_k)}\right| \leq \rho < 1 \tag{25}$$

for all $x_k \in X$ and for all $\bar{p}_k \in P$. Then,

$$\begin{aligned} &|p - p_k| \leq \\ &\quad \rho(|p - p_{k-1}| + l_g(1 + l_h)|\gamma||x - x_k| + \epsilon_\eta). \end{aligned} \tag{26}$$

Note that the following equality holds.

$$|x(t) - x_k(t)| \leq \epsilon_0 \mathrm{e}^{l_f t} + l_f \int_0^t \mathrm{e}^{l_f(t-\tau)}|p - p_k| \mathrm{d}\tau. \tag{27}$$

Substituting (27) into (26) yields

$$\begin{aligned} &|p - p_k| - \rho l_f l_g(1 + l_h)|\gamma| \int_0^t \mathrm{e}^{l_f(t-\tau)}|p - p_k|\mathrm{d}\tau \leq \\ &\quad \rho\big(|p - p_{k-1}| + l_g(1 + l_h)|\gamma|\epsilon_0 \mathrm{e}^{l_f t} + \epsilon_\eta\big). \end{aligned}$$

As $\lambda > l_f$, we obtain

$$\begin{aligned} &(1 - \rho l_f l_g(1 + l_h)|\gamma| \frac{1 - \mathrm{e}^{(l_f - \lambda)T}}{\lambda - l_f})|p - p_k|_\lambda \leq \\ &\quad \rho\big(|p - p_{k-1}|_\lambda + l_g(1 + l_h)|\gamma|\epsilon_0 + \epsilon_\eta\big). \end{aligned} \tag{28}$$

Let us define

$$\begin{aligned} \bar{\rho} &= \frac{\rho}{1 - \rho l_f l_g(1 + l_h)|\gamma| \dfrac{1 - \mathrm{e}^{(l_f - \lambda)T}}{\lambda - l_f}} \\ \bar{\epsilon} &= \bar{\rho}\big(l_g(1 + l_h)|\gamma|\epsilon_0 + \epsilon_\eta\big). \end{aligned}$$

Equation (28) becomes

$$|p - p_k|_\lambda \leq \bar{\rho}|p - p_{k-1}|_\lambda + \bar{\epsilon}.$$

We are now at a position to summary the robustness and convergence result.

Theorem 4. Consider the system consisting of the transmitters (4) and (23), and the receivers (6) and (24), satisfying Assumptions 1−4, 5′ and 6. Let update law (12) be applied with the learning gain chosen to satisfy (25). Then, the same results as in Theorem 1 are obtained.

The scheme given by (23) and (24) just uses the composition of two nonlinear functions. For security enhancement, however, multiple composite functions can be applied in the form of

$$\left\{ \begin{aligned} s &= g(x, s^1) \\ s^1 &= h_1(x, s^2) \\ &\cdots \\ s^{m-1} &= h_{m-1}(x, s^m) \\ s^m &= h_m(x, p). \end{aligned} \right. \tag{29}$$

The theoretical analysis for the case of multiple composition follows the similar lines to the derivations for Theorem 4, where the nonlinear functions used for composition are required to be Lipschitz in their arguments. It should be to noted that the composite function is Lipschitz as the functions used to form the composition are Lipschitz in their arguments.

5 Case studies

Consider the following unified chaotic system proposed in [19],

$$\begin{aligned} \dot{x}_1 &= (25\alpha + 10)(x_2 - x_1) \\ \dot{x}_2 &= (28 - 35\alpha)x_1 - x_1 x_3 + (29\alpha - 1)x_2 \\ \dot{x}_3 &= x_1 x_2 - \frac{\alpha + 8}{3} x_3. \end{aligned}$$

The message masking is carried out by calculating with the nonlinear function as

$$s = \frac{1}{2\tanh\big(\varrho(x, p)\big) + 1} \tag{30}$$

$$\varrho(x, p) = c_1 x_3 + (c_2 x_1 + c_3)p \tag{31}$$

where p indicates the plaintext, and $c_i, i = 1, 2, 3$, are adjustable parameters.

In the chaotic system, we replace α with p, and the system becomes

$$\dot{x}_1 = (25p + 10)(x_2 - x_1)$$
$$\dot{x}_2 = (28 - 35p)x_1 - x_1x_3 + (29p - 1)x_2$$
$$\dot{x}_3 = x_1x_2 - \frac{p+8}{3}x_3.$$

For the learning law (12), it is easy to choose the learning gain according to the convergence condition (16).

$$\frac{\partial g}{\partial p} = \frac{1}{2}\mathrm{sech}^2\big(\varrho(x,p)\big)(c_2x_1 + c_3).$$

Due to the boundedness of the function sech, it is easy for us to choose γ. In view of (16), we have to choose c_2 and c_3 such that $c_2x_1 + c_3 > 0$.

We shall test the iterative learning based secure communication scheme for the settings as

$$x^0 = [10, 20, 30]^{\mathrm{T}}$$
$$c_1 = \frac{1}{100}, c_2 = \frac{1}{100}, c_3 = 1$$
$$m_{\min} = 0.4, m_{\max} = 0.9.$$

Our scheme does not need the message to be differentiable, which can be discontinuous ones tailored for digital communication.

The plaintext is chosen to be a square wave on the interval $[0, 6]$, i.e., $T = 6$. The transmitted signal is generated by (30), which is shown in Fig. 1. Note that our scheme does not need the knowledge about $x_1(t), x_2(t), x_3(t), t \in (0, T]$. In order to recovery the message from the transmitted signal, the learning law (12) is applied with the setting of $p_0(t) = 0,\ t \in [0, T]$. Define the performance index as $J_k = \sup_{t\in[0,T]}|p(t) - p_k(t)|$. Fig. 2 shows the convergence rate comparison with different learning gains of $\gamma = 0.5, 1.5$ and 3. It verifies that a larger learning gain could lead to a faster convergence rate. With the choice of $\gamma = 3$, the performance of $J_k < 10^{-5}$ is achieved at the cycle $k = 15$. The recovered message is shown in Fig. 3.

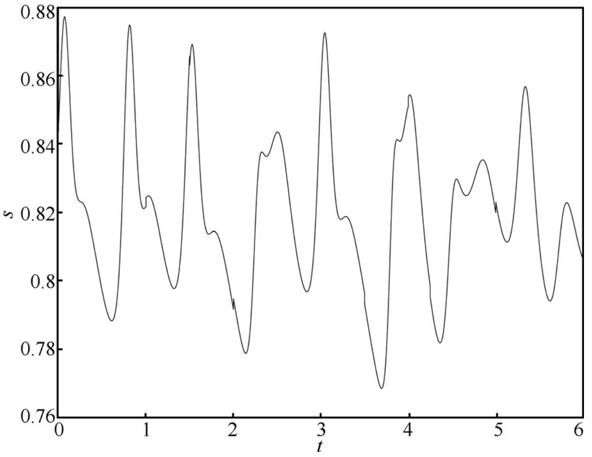

Fig. 1 The transmitted signal generated by (30)

The robustness of a learning algorithm is crucial due to its iteration nature. We then examine the robustness of the scheme to initial condition error and measurement noise. Let us set the initial condition to be $x^0 + \frac{1}{10}[1, -1, 1]^{\mathrm{T}}$, where x^0 is set to be the same as that in generating the transmitted signal, $\eta_k = \frac{1}{1000} \times (2\mathrm{rand} - 1)$, and the rand is a random scalar, chosen from a uniform distribution on the interval $(0, 1)$. The recovery result obtained through 100 iterations is shown in Fig. 4. It is observed from Fig. 4 that our learning scheme will not be divergent in the presence of the uncertainties, but robust to the uncertainties.

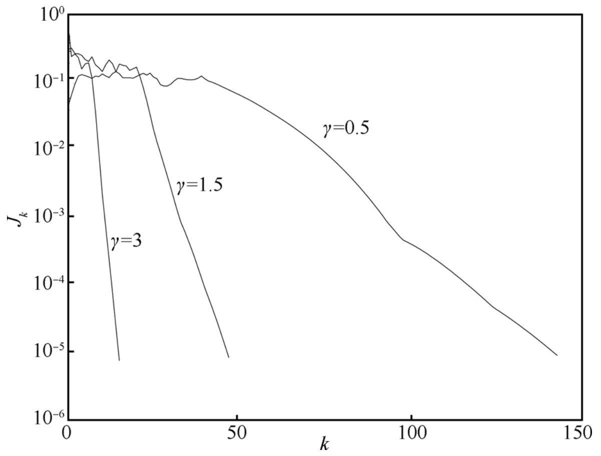

Fig. 2 Convergence rate comparison with different learning gains

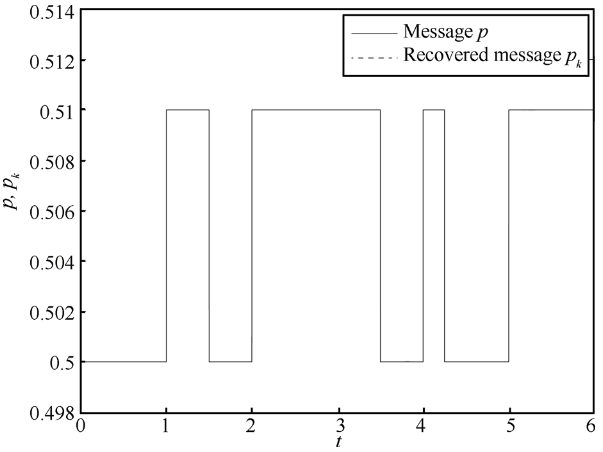

Fig. 3 Message recovery

The recovery performance with the proposed techniques for enhancing security is now examined. Let us replace the parameter α with the signal s, instead of the message signal p. Other settings remain the same. The numerical results are shown in Figs. 5 and 6. Fig. 5 depicts the convergence rate comparison with different learning gains. The performance of $J_k < 10^{-5}$ is achieved at the cycle $k = 20$ as we choose $\gamma = 3$. Robustness of the scheme to initial condition error and measurement noise is examined in Fig. 6.

The following composite function is then used to generate the signal s as

$$s = \frac{1}{2\big(\tanh\big(\varrho(x, s^1)\big) + 1\big)} \tag{32}$$

$$s^1 = \frac{1}{2\big(\tanh\big(\varrho(x, p)\big) + 1\big)} \tag{33}$$

while other settings remain the same. The simulation results are shown in Figs. 7 and 8. The convergence rate comparison with different learning gains of $\gamma = 2, 4$ and 6 is given in Fig. 7. $J_k < 10^{-5}$ is achieved at the cycle $k = 159$ as $\gamma = 6$ is chosen. It is clarified that more iterations are needed to achieve the same performance as high nonlinearity is included. Fig. 8 shows the robustness of the scheme to initial condition error and measurement noise.

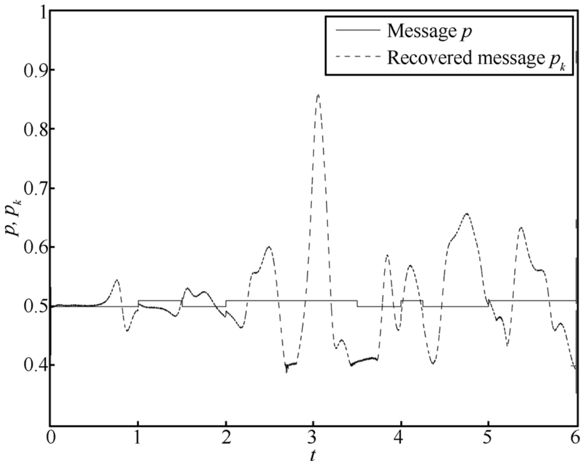

Fig. 4 Robustness to presence of initial condition error and measurement error

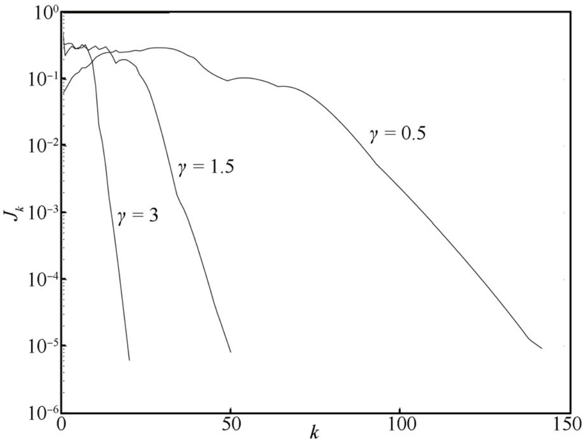

Fig. 5 Convergence rate comparison. The parameter α is replaced by the signal s

6 Conclusions

The iterative learning perspective on secure communication is presented, in this paper, allowing us to apply a nonlinear mechanism for masking without inversion computing for decryption. In addition, the masking can be applied jointly with parameter modulation. The convergence condition of the learning algorithm has been derived, by which the learning gain can be chosen. The technique by increasing nonlinearities in masking is presented for enhancing security, and the learning algorithm has been shown to work well. The computer simulation has been carried out and numerical results have been provided to show the effectiveness and feasibility of the developed method.

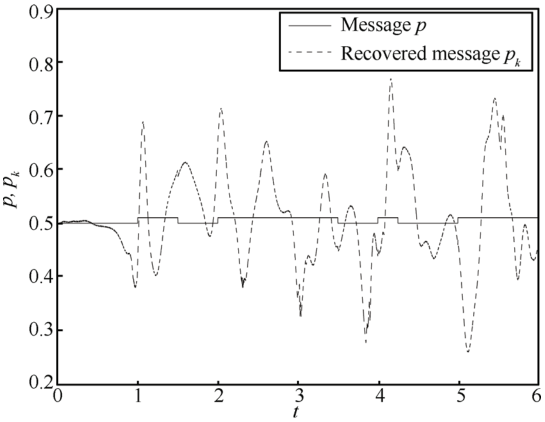

Fig. 6 Robustness to presence of initial condition error and measurement error. The parameter α is replaced by the signal s

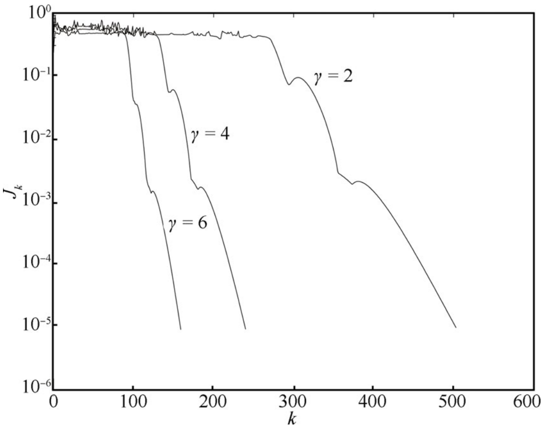

Fig. 7 Convergence rate comparison. The transmitted signal is generated by (32)

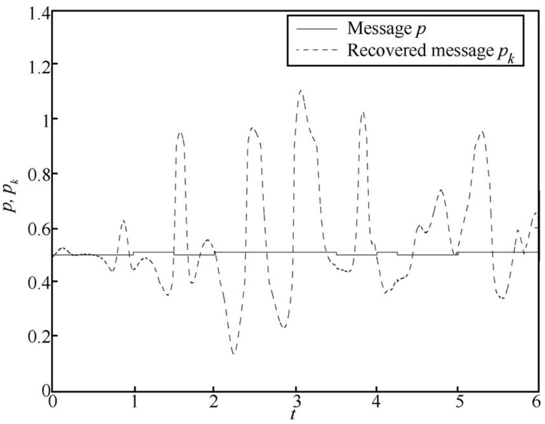

Fig. 8 Robustness to presence of initial condition error and measurement error. The transmitted signal is generated by (32)

Appendix

A. Proof of Lemma 1

There are three possible cases which we should considers for proving (15).

Case $\bar{b}^1 \leq b \leq \bar{b}^2$: It follows that $\mathrm{sat}(b) = b$ and $|a - \mathrm{sat(b)}|^r = |a - b|^r$. Hence, (15) is true for this case.

Case $b > \bar{b}^2$: It follows that $\mathrm{sat}(b) = \bar{b}^2$ and $a - \bar{b}^2 > a - b$. Since $\bar{b}^1 < a < \bar{b}^2$, one has $a - \bar{b}^2 < 0$ and $a - b < 0$, which results in $|a - \bar{b}^2| < |a - b|$ and $|a - \bar{b}^2|^r < |a - b|^r$ as $r > 0$. Hence, (15) also holds for this case.

Case $b < \bar{b}^1$: It follows that $\mathrm{sat}(b) = \bar{b}^1$ and $a - \bar{b}^1 < a - b$. Since $\bar{b}^1 < a < \bar{b}^2$, one has $a - \bar{b}^1 > 0$ and $a - b > 0$, which results in $|a - \bar{b}^1| < |a - b|$ and $|a - \bar{b}^1|^r < |a - b|^r$ as $r > 0$. Hence, (15) holds as well for this case.

Inequality (15) is true for all three cases.

B. Proof of Theorem 1

It follows by the update law (12) that

$$\begin{aligned}
&p - p_k = p - \mathrm{sat}(p_{k-1}) - \gamma(s - s_k) - \eta_k = \\
&\quad p - \mathrm{sat}(p_{k-1}) - \gamma\big(g(x, p) - g(x_k, p) + \\
&\quad g(x_k, p) - g(x_k, p_k)\big) - \eta_k. \qquad \text{(B1)}
\end{aligned}$$

By appealing to the mean value theorem, there exists $\bar{p}_k = p + (1 - \xi)(p_k - p), \xi \in (0, 1)$, which lies on the line segment jointing p_k and p, such that

$$g(x_k, p) - g(x_k, p_k) = g_p(x_k, \bar{p}_k)(p - p_k).$$

Equation (B1) can be rewritten as

$$\begin{aligned}
p - p_k = p - \mathrm{sat}\big(p_{k-1}\big) - \gamma\big(g(x, p) - g(x_k, p) + \\
g_p(x_k, \bar{p}_k)(p - p_k)\big) - \eta_k
\end{aligned}$$

which implies that

$$\begin{aligned}
&p - p_k = \frac{1}{1 + \gamma g_p(x_k, \bar{p}_k)}\big(p - \mathrm{sat}(p_{k-1}) - \\
&\quad \gamma\big(g(x, p) - g(x_k, p)\big) - \eta_k\big). \qquad \text{(B2)}
\end{aligned}$$

Taking absolute values on both sides of (B2) yields

$$\begin{aligned}
|p - p_k| \leq \left|\frac{1}{1 + \gamma g_p(x_k, \bar{p}_k)}\right| \big(|p - \mathrm{sat}\big(p_{k-1}\big)| + \\
|\gamma||g(x, p) - g(x_k, p)| + |\eta_k|\big).
\end{aligned}$$

By Lemma 1, the saturation feature results in

$$\begin{aligned}
|p - p_k| \leq \left|\frac{1}{1 + \gamma g_p(x_k, \bar{p}_k)}\right| \big(|p - p_k| + \\
|\gamma||g(x, p) - g(x_k, p)| + |\eta_k|\big).
\end{aligned}$$

Using (16) and by Assumptions 2 and 5, we have

$$|p - p_k| \leq \rho(|p - p_{k-1}| + l_g|\gamma||x - x_k| + \epsilon_\eta). \qquad \text{(B3)}$$

To proceed, we need to evaluate the term $|x - x_k|$ on the right hand side of (B3). Integrating both sides of (4) and (6), the integral expression can be written as

$$x(t) - x_k(t) = x(0) - x_k(0) + \int_0^t \big(f(x, p) - f(x_k, p_k)\big)\mathrm{d}\tau.$$

It follows by Assumption 4 that

$$\begin{aligned}
&|x(t) - x_k(t)| \leq \\
&\quad |x(0) - x_k(0)| + \int_0^t |f(x, p) - f(x_k, p_k)|\mathrm{d}\tau \leq \\
&\quad \epsilon_0 + \int_0^t l_f(|x - x_k| + |p - p_k|)\mathrm{d}\tau.
\end{aligned}$$

Applying Bellman-Gronwall Lemma gives rise to

$$|x(t) - x_k(t)| \leq \epsilon_0 \mathrm{e}^{l_f t} + l_f \int_0^t \mathrm{e}^{l_f(t - \tau)}|p - p_{k-1}|\mathrm{d}\tau. \qquad \text{(B4)}$$

Substituting (B4) into (B3) leads to

$$\begin{aligned}
&|p - p_k| \leq \rho\bigg(|p - p_{k-1}| + \\
&\quad l_f l_g|\gamma| \int_0^t \mathrm{e}^{l_f(t - \tau)}|p - p_k|\mathrm{d}\tau + l_g|\gamma|\mathrm{e}^{l_f t}\epsilon_0 + \epsilon_\eta\bigg). \qquad \text{(B5)}
\end{aligned}$$

Multiplying both sides of (B5) by $\mathrm{e}^{-\lambda t}(\lambda > 0)$ yields

$$\begin{aligned}
&\mathrm{e}^{-\lambda t}|p - p_k| \leq \\
&\quad \rho\bigg(\mathrm{e}^{-\lambda t}|p - p_{k-1}| + l_f l_g|\gamma| \int_0^t \mathrm{e}^{(l_f - \lambda)(t - \tau)}\mathrm{e}^{-\lambda\tau} \\
&\quad |p - p_k|\mathrm{d}\tau + l_g|\gamma|\mathrm{e}^{(l_f - \lambda)t}\epsilon_0 + \mathrm{e}^{-\lambda t}\epsilon_\eta\bigg).
\end{aligned}$$

Taking supremum for $t \in [0, T]$ and $\lambda > l_f$, we have

$$\begin{aligned}
&\mathrm{e}^{-\lambda t}|p - p_k| \leq \rho\bigg(\sup_{t \in [0, T]}\{\mathrm{e}^{-\lambda t}|p - p_{k-1}|\} + \\
&\quad l_f l_g|\gamma| \int_0^t \mathrm{e}^{(l_f - \lambda)(t - \tau)} \sup_{\tau \in [0, T]}\{\mathrm{e}^{-\lambda\tau}|p - p_k|\}\mathrm{d}\tau + \\
&\quad l_g|\gamma|\epsilon_0 + \epsilon_\eta\bigg)
\end{aligned}$$

which implies that

$$\begin{aligned}
&\sup_{t \in [0, T]}\{\mathrm{e}^{-\lambda t}|p - p_k|\} \leq \\
&\quad \rho\bigg(\sup_{t \in [0, T]}\{\mathrm{e}^{-\lambda t}|p - p_{k-1}|\} + l_f l_g|\gamma|\frac{1 - \mathrm{e}^{(l_f - \lambda)T}}{\lambda - l_f} \times \\
&\quad \sup_{\tau \in [0, T]}\{\mathrm{e}^{-\lambda\tau}|p - p_k|\} + l_g|\gamma|\epsilon_0 + \epsilon_\eta\bigg).
\end{aligned}$$

By the definition of the λ-norm, we have

$$\begin{aligned}
&\left(1 - \rho l_f l_g|\gamma|\frac{1 - \mathrm{e}^{(l_f - \lambda)T}}{\lambda - l_f}\right)|p - p_k|_\lambda \leq \\
&\quad \rho(|p - p_{k-1}|_\lambda + l_g|\gamma|\epsilon_0 + \epsilon_\eta). \qquad \text{(B6)}
\end{aligned}$$

Let us define

$$\bar{\rho} = \frac{\rho}{1 - \rho l_f l_g|\gamma|\dfrac{1 - \mathrm{e}^{(l_f - \lambda)T}}{\lambda - l_f}}$$

$$\bar{\epsilon} = \bar{\rho}(l_g|\gamma|\epsilon_0 + \epsilon_\eta).$$

Equation (B6) becomes

$$|p - p_k|_\lambda \leq \bar{\rho}|p - p_{k-1}|_\lambda + \bar{\epsilon}. \qquad \text{(B7)}$$

Since $0 \leq \rho < 1$, it is possible to have a sufficiently large $\lambda(> l_f)$ such that

$$1 - \rho l_f l_g |\gamma| \frac{1 - \mathrm{e}^{(l_f - \lambda)T}}{\lambda - l_f} > 0$$

and

$$0 \leq \bar{\rho} < 1.$$

Inequality (40) indicates a contraction in $|p - p_k|_\lambda$. Therefore, as the iteration increases,

$$\limsup_{k \to \infty} |p - p_k|_\lambda \leq \frac{\bar{\epsilon}}{1 - \bar{\rho}}.$$

By the inequality $\sup_{t \in [0,T]} |p - p_k| \leq \mathrm{e}^{\lambda T} |p - p_k|_\lambda$, the theorem follows.

C. Proof of Theorem 2

From the learning law, we obtain

$$\begin{aligned} p - p^*_{k+1} = {} & p - \mathrm{sat}(p^*_k) - \gamma(s - s_k) - \eta_k = \\ & p - \mathrm{sat}(p^*_k) - \gamma\big(g(x, p) - g(x_k, p_k)\big) - \eta_k = \\ & p - p_k - \gamma\big(g(x, p) - g(x_k, p) + g(x_k, p) - \\ & g(x_k, p_k)\big) - \eta_k. \end{aligned}$$

Note that $g(x_k, p) - g(x_k, p_k) = g_p(x_k, \bar{p}_k)(p - p_k)$, $\bar{p}_k = p + (1 - \xi)(p_k - p), 0 < \xi < 1$. We obtain

$$\begin{aligned} & p - p^*_{k+1} = \\ & \quad p - p_k - \gamma\big(g(x, p) - g(x_k, p) + g_p(x_k, \bar{p}_k)(p - p_k)\big) - \eta_k = \\ & \quad p - p_k - \gamma\big(g(x, p) - g(x_k, p) + \\ & \quad g_p(x_k, \bar{p}_k)(p - p_k)\big) - \eta_k. \end{aligned}$$

Hence,

$$\begin{aligned} & p - p^*_{k+1} = \\ & \big(1 - \gamma g_p(x_k, \bar{p}_k)\big)(p - p_k) - \gamma\big(g(x, p) - g(x_k, p)\big) - \eta_k. \end{aligned}$$

Taking norms

$$\begin{aligned} |p - p^*_{k+1}| \leq {} & |1 - \gamma_k g_p(x_k, \bar{p}_k)||p - p_k| + \\ & |\gamma||g(x, p) - g(x_k, p)| + |\eta_k| \end{aligned}$$

and setting $|1 - \gamma g_p(x_k, \bar{p}_k)| \leq \rho < 1$, we have

$$|p - p^*_{k+1}| \leq \rho |p - p_k| + b_\gamma l_g |x - x_k| + \epsilon_\eta.$$

Note that $|p - p_k| = |p - \mathrm{sat}(p^*_k)| \leq |p - p^*_k|$. Then,

$$|p - p^*_{k+1}| \leq \rho |p - p^*_k| + b_\gamma l_g |x - x_k| + \epsilon_\eta.$$

Using the estimation for $|x - x_k|$, we have

$$\begin{aligned} & |p - p^*_{k+1}| \leq \\ & \quad \rho |p - p_k| + b_\gamma l_g [\epsilon_0 \mathrm{e}^{l_f t} + \\ & \quad l_f \int_0^t \mathrm{e}^{l_f (t - \tau)} |p - p_k| \mathrm{d}\tau] + \epsilon_\eta \leq \\ & \quad \rho |p - p^*_k| + b_\gamma l_g l_f \int_0^t \mathrm{e}^{l_f (t - \tau)} |p - p^*_k| \mathrm{d}\tau + \\ & \quad b_\gamma l_g \epsilon_0 \mathrm{e}^{l_f t} + \epsilon_\eta. \end{aligned}$$

As $\lambda > l_f$,

$$\begin{aligned} & |p - p^*_{k+1}|_\lambda \leq \\ & \quad \left(\rho + b_\gamma l_g l_f \frac{1 - \mathrm{e}^{(l_f - \lambda)T}}{\lambda - l_f}\right) |p - p^*_k|_\lambda + \\ & \quad b_\gamma l_g \epsilon_0 + \epsilon_\eta. \end{aligned}$$

Let us denote that $\bar{\rho} = \rho + b_\gamma l_g l_f \frac{1 - \mathrm{e}^{(l_f - \lambda)T}}{\lambda - l_f}$ and $\bar{\epsilon} = b_\gamma l_g \epsilon_0 + \epsilon_\eta)$. Then,

$$\limsup_{k \to \infty} |p - p_k|_\lambda \leq \frac{\bar{\epsilon}}{1 - \bar{\rho}}.$$

□

References

[1] L. M. Pecora, T. L. Carroll. Synchronization in chaotic systems. *Physical Preview Letters*, vol. 64, no. 8, pp. 821–824, 1990.

[2] K. M. Cuomo, A. V. Oppenheim. Circuit implementation of synchronized chaos with applications to communications. *Physical Review Letters*, vol. 71, no. 1, pp. 65–68, 1993.

[3] G. R. Chen, X. N. Dong. *From Chaos to Order: Methodologies, Perspectives and Applications*, Singapore: World Scientific, 1998.

[4] A. L. Fradkov, R. J. Evans. Control of chaos: Methods and applications in engineering. *Annual Reviews in Control*, vol. 29, no. 1, pp. 33–56, 2005.

[5] T. Yang, L. O. Chua. Secure communication via chaotic parameter modulation. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 43, no. 9, pp. 817–819, 1996.

[6] N. J. Corron, D. W. Hahs. A new approach to communications using chaotic signals. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 44, no. 5, pp. 373–382, 1997.

[7] L. Kocarev, U. Parlitz. General approach for chaotic synchronization with applications to communication. *Physical Preview Letters*, vol. 74, no. 25, pp. 5028–5031, 1995.

[8] T. Yang, C. W. Wu, L. O. Chua. Cryptography based on chaotic systems. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 44, no. 5, pp. 469–472, 1997.

[9] H. Nijmeijer, I. M. Y. Mareels. An observer looks at synchronization. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 44, no. 10, pp. 882–890, 1997.

[10] H. Huijberts, H. Nijmeijer, R. Willems. System identification in communication with chaotic systems. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 47, no. 6, pp. 800–808, 2000.

[11] S. Arimoto, S. Kawamura, F. Miyazaki. Bettering operation of robots by learning. *Journal of Robotic Systems*, vol. 1, no. 2, pp. 123–140, 1984.

[12] D. A. Bristow, M. Tharayil, A. G. Alleyne. A survey of iterative learning control. *IEEE Control Systems Magazine*, vol. 26, no. 3, pp. 96–114, 2006.

[13] M. X. Sun, D. W. Wang. Closed-loop iterative learning control for non-linear systems with initial shifts. *International Journal of Adaptive Control and Signal Processing*, vol. 16, no. 7, pp. 515–538, 2002.

[14] D. P. Huang, J. X. Xu, V. Venkataramanan, T. C. T. Huynh. High-performance tracking of piezoelectric positioning stage using current-cycle iterative learning control with gain scheduling. *IEEE Transactions on Industrial Electronics*, vol. 61, no. 2, pp. 1085–1098, 2014.

[15] M. X. Sun. Chaotic communication systems: An iterative learning perspective. In *Proceedings of the International Conference on Electrical and Control Engineering*, IEEE, Wuhan, China, pp. 573–577, 2010.

[16] U. Feldmann, M. Hasler, W. Schwaz. Communication by chaotic signals: The inverse system approach. *International Journal of Circuit Theory and Applications*, vol. 24, no. 5, pp. 551–579, 1996.

[17] H. Zhou, X. T. Ling. Problems with the chaotic inverse system encryption approach. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 44, no. 3, pp. 268–271, 1997.

[18] Y. Zheng, G. R. Chen, C. Y. Zhu. A system inversion approach to chaos-based secure speech communication. *International Journal of Bifurcation and Chaos*, vol. 15, no. 8, pp. 2569–2582, 2005.

[19] J. H. Lü, G. R. Chen, D. Z. Cheng, S. Celikovsky. Bridge the gap between the Lorenz system and the Chen system. *International Journal of Bifurcation and Chaos*, vol. 12, no. 12, pp. 2917–2926, 2002.

Ming-Xuan Sun received the B. Eng. degree from the Xi′an University of Technology, China in 1982, the M. Eng. degree from Beijing Institute of Technology, China in 1987, and the Ph. D. degree from the Nanyang Technological University, Singapore in 2002.

From 1982 to 1984, he was with the Hefei General Machinery Research Institute, China. He joined the Department of Electrical Engineering, Xi′an Institute of Technology, China in 1987. He held research positions at the Nanyang Technological University and the National University of Singapore, Singapore from 2001 to 2004. Since 2004, he has been with the Zhejiang University of Technology, China. He is currently a professor of the College of Information Engineering, Zhejiang University of Technology.

His research interests include iterative learning control, repetitive control and their applications.

E-mail: mxsun@zjut.edu.cn (Corresponding author)
ORCID iD: 0000-0003-2553-6154