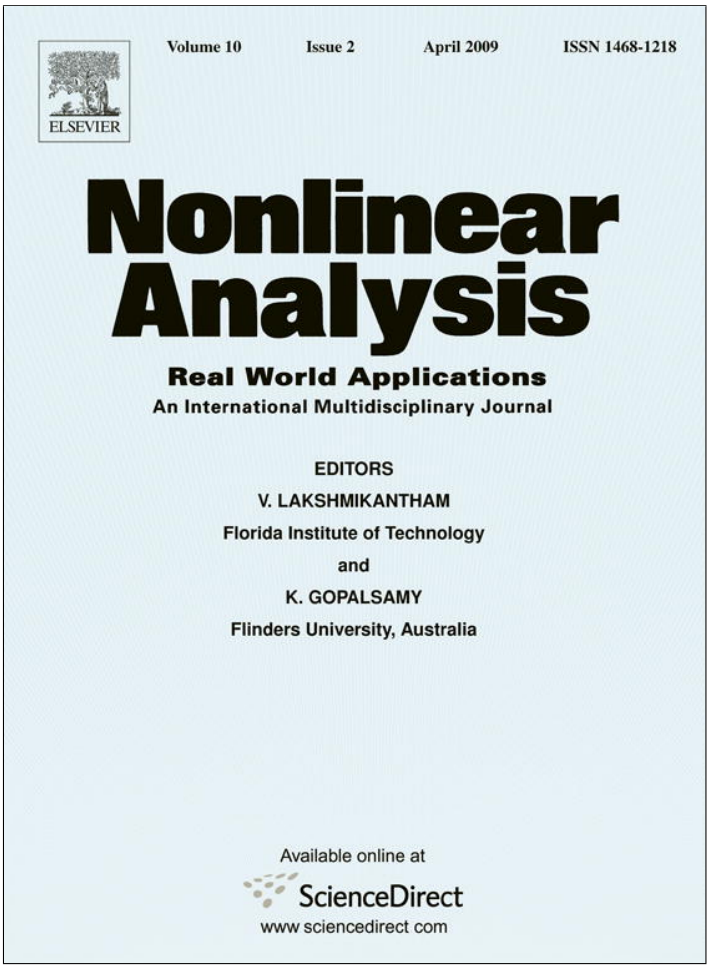

Available online at www.sciencedirect.com
ScienceDirect
Nonlinear Analysis: Real World Applications 10 (2009) 869–880
Nonlinear Analysis
Real World Applications
www.elsevier.com/locate/nonrwa

Asymptotic synchronization of modified logistic hyper-chaotic systems and its applications

Shu-Ming Chang[b], Ming-Chia Li[b], Wen-Wei Lin[a,*]

[a] *Department of Mathematics, National Tsing Hua University, Hsinchu, 300, Taiwan*
[b] *Department of Applied Mathematics, National Chiao Tung University, Hsinchu, 300, Taiwan*

Received 15 August 2007; accepted 6 November 2007

Abstract

In this paper, we propose a Modified Logistic Map (MLM) and give a theoretical proof to show that the MLM is a chaotic map according to Devaney's definition. The MLM not only has no chaotic window but is also uniformly distributed in [0, 1] for $\gamma \geq 4$. Furthermore, on the basis of the MLMs, we establish a Modified Logistic Hyper-Chaotic System (MLHCS) and apply the MLHCS to develop a symmetric cryptography algorithm, Asymptotic Synchronization of the Modified Logistic Hyper-Chaotic System (ASMLHCS). In our numerical simulation, we analyze the spectra of waveforms of sequences generated from the MLM, showing that the orbit forms a uniform distribution in [0, 1]. In addition, we compute the Poincaré recurrences which indicate that the MLM possesses a positive topological entropy.

Keywords: Modified logistic map; No window; Hyper-chaos; Asymptotic synchronization; Secure communication; Poincaré recurrences

1. Introduction

A logistic map of the form

$$\overline{x} = \gamma x(1 - x) \tag{1.1}$$

is an essential quadratic map in discrete dynamics which has been extensively studied, not only theoretically but also numerically, by mathematicians, physicists and biologists. It is well known that the logistic map has chaotic behavior for $3.57 < \gamma \leq 4$ [6,7,9]. However, the set of chaotic windows is open and dense [4]; that is, the set of visualized chaos is small and sparse for $\gamma \in (3.57, 4)$. On the other hand, the logistic map is also proved to be chaotic on an invariant Cantor set for all $\gamma > 4$ which is unstable [11,17].

Pecora and Carrol [14] have shown that a chaotic system (response system) can be synchronized with a separated chaotic system (drive system), provided that the conditional Lyapunov exponents of the difference equations between the drive and response systems are all negative. In secure communication, the chaotic signals are used as

* Corresponding author. Tel.: +886 3 573 1057; fax: +886 3 571 8949.
E-mail addresses: smchang@math.nctu.edu.tw (S.-M. Chang), mcli@math.nctu.edu.tw (M.-C. Li), wwlin@math.nthu.edu.tw (W.-W. Lin).

1468-1218/$ - see front matter
doi:10.1016/j.nonrwa.2007.11.010

masking streams to carry information which can be recovered through chaotic synchronization behavior, between the transmitter (drive system) and receiver (response system).

Sobhy and Shehata [21] attacked the chaotic secure system by reconstructing the map with the output sequence. Because of the unique map pattern of each single chaotic system, it is easy to distinguish from the other chaotic systems and rebuild the equations. MATLAB routines are used to approximate the parameters. Once the parameters are found, the secure information is recovered.

Therefore, many papers focus on enhancing the complexity of the output sequence. Heidari-Bateni and McGillem [8] use a chaotic map to initialize another chaotic map. Utilizing a multi-system, several chaotic maps are switched by the specific mechanism [10] or combined into a chaotic system chain [23]. Peng et al. [15] combine the above two approaches.

In this paper, we propose a robust map, the Modified Logistic Map (MLM). The MLM is a chaotic map by the definition of Devaney and invariant in [0, 1]. Furthermore, the MLM has *no window*. In numerical computation, we compute Poincaré recurrences to indicate the chaotic phenomena of the MLM. On the basis of two MLMs, we establish a Modified Logistic Hyper-Chaotic System (MLHCS). We then develop a symmetric cryptography algorithm, Asymptotic Synchronization of the Modified Logistic Hyper-Chaotic System (ASMLHCS), consisting of two MLHCSs. There are two parts in the ASMLHCS, namely the asymptotic synchronization phase and the encryption/decryption phase. The details will be introduced in later sections.

The rest of the paper is organized as follows. In Section 2, we present an MLM and prove that the map has chaos. In Section 3, we utilize the spectra of waveforms and Poincaré recurrences to study the properties of the MLM. In Section 4, the MLHCS will be proposed and its applications investigated. In Section 5, we develop a symmetric cryptography algorithm consisting of two MLHCSs. Finally, concluding remarks are made in Section 6.

2. Modified logistic map: Devaney's chaos

For $\gamma > 0$, we define the Modified Logistic Map (MLM) $f_\gamma(x) : [0, 1] \to [0, 1]$ by

$$f_\gamma(x) = \begin{cases} \gamma x(1-x) \pmod 1, & \text{if } x \in [0,1] \setminus (\eta_1, \eta_2), \\ \dfrac{\gamma x(1-x) \pmod 1}{\frac{\gamma}{4} \pmod 1}, & \text{if } x \in (\eta_1, \eta_2), \end{cases} \tag{2.1}$$

where $\eta_1 = \frac{1}{2} - \sqrt{\frac{1}{4} - \frac{[\frac{\gamma}{4}]}{\gamma}}$, $\eta_2 = \frac{1}{2} + \sqrt{\frac{1}{4} - \frac{[\frac{\gamma}{4}]}{\gamma}}$ and $[z]$ is the greatest integer less than or equal to z.

For $\gamma \le 4$, we can easily observe that $f_\gamma(x)$ is equivalent to the classical logistic map (1.1) at $\gamma = 4$. It is well known that the classical logistic map has chaotic behavior for $3.57 < \gamma \le 4$. Consequently, the sequence generated by the MLM never settles down to a fixed point or a periodic orbit, instead of the aperiodic long-time behavior. However, from the bifurcation diagram [5], we see that the attractors generated by the classical logistic map route from period doubling to chaos (strange attractor). The range of the strange attractors becomes larger and larger, as γ increases from 3.57 to 4. For $\gamma = 4$, the length of the strange attractor is 1. In fact, the attractor of a chaotic window visually forms periodic points, and has been proved to be open and dense.

As the MLM has no chaotic windows for $\gamma < 4$, which is suitable for a chaotic mask in secure communication, in the following we shall show that the MLM also has chaotic behavior according to Devaney's definition [6] for $\gamma \ge 4$. In these cases the lengths of strange attractors are always 1 and the chaotic behavior is topologically equivalent to that of $\gamma = 4$. In other words, for $\gamma > 0$, the MLM has no chaotic windows which produce a large key space in secure communication.

Fig. 2.1 plots a modified logistic map with $\gamma = 10$ which is a piecewise monotonic transformation.

Definition 1. Let $f : I \to I$ be a map, where I is a closed interval. We say that f exhibits *Devaney's chaos* on I if the following conditions are satisfied:

1. the set of periodic points is dense in I;
2. the map f is *topologically transitive*, i.e., for any given pair of nonempty open sets U and V in I, there is a positive integer n such that $f^n(U) \cap V \neq \emptyset$; and

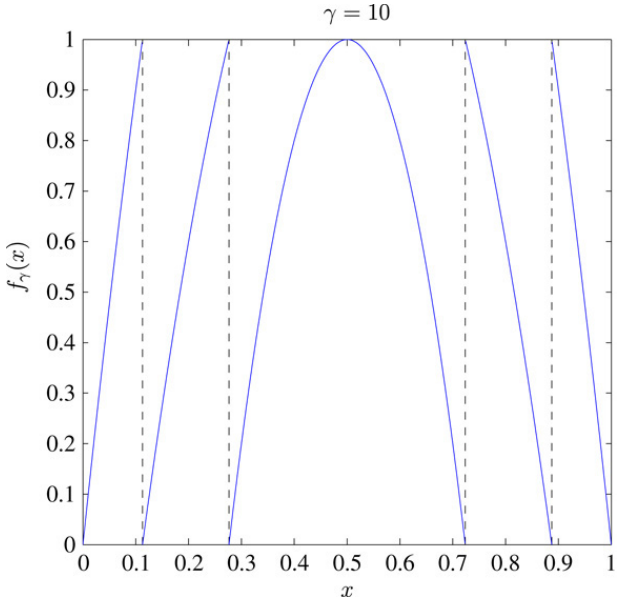

Fig. 2.1. MLM with $\gamma = 10$.

3. the map f has *sensitive dependence on initial conditions*; i.e., there exists $\alpha > 0$ such that for any $x \in I$ and any $\epsilon > 0$, there are $y \in I$ and $n \in \mathbb{N}$ such that $|x - y| < \epsilon$ and $|f^n(x) - f^n(y)| > \alpha$.

We also need the following definition. For a C^3 map $g : I \to I$, where I is an interval, the *Schwarzian derivative* of g is defined by

$$S_g(x) = \frac{g'''(x)}{g'(x)} - \frac{3}{2}\left(\frac{g''(x)}{g'(x)}\right)^2$$

for $x \in I$ with $g'(x) \neq 0$. By the chain rule, one has $S_g < 0$ which implies $S_{g^2} < 0$. Hence,

$$\text{if } S_g < 0, \quad \text{then } S_{g^n} < 0 \quad \text{for all } n \geq 1. \tag{2.2}$$

Moreover, $S_g < 0$ implies that g' cannot have a positive local minimum or a negative local maximum. Indeed, if c is a critical point of g', then $\frac{g'''(c)}{g'(c)} = S_g(c) < 0$ and hence $g'''(c)$ and $g'(c)$ have opposite signs. Therefore, by the continuity of g', we have that if $g' \neq 0$ and $S_g < 0$ on $[a, b]$, then for any $x \in (a, b)$,

$$\text{either } g'(x) > \min\{g'(a), g'(b)\} > 0 \quad \text{or} \quad g'(x) < \max\{g'(a), g'(b)\} < 0. \tag{2.3}$$

We now return to our study on the model f_γ in (2.1) and show the existence of Devaney's chaos.

Theorem 2.1. *If $\gamma \geq 4$, then f_γ exhibits Devaney's chaos on* $[0, 1]$.

Proof. Without loss of generality, we assume that $4 < \gamma < 8$. For convenience, we write $f = f_\gamma$. Then there are four fixed points $0 < A < B < C$. There is a point B_- such that $A < B_- < B$ and $f(B_-) = B$. Let $k = [\gamma/4] - 1$ and $J = \{x \in [B_-, B] : f^n(x) \in [B_-, B] \text{ for some integer } n \geq 1\}$. For $x \in J$, define $\tau(x) = \min\{n \in \mathbb{N} : f^n(x) \in [B_-, B]\}$. Then $\tau(x)$ is well defined.

First, we claim

$$|(f^{\tau(x)})'(x)| > 1 \quad \text{for all } x \in J. \tag{2.4}$$

For $n \geq 1$, let $I_n = \{x \in (1/2, B] : \tau(x) = n\}$ and $\hat{I}_n = \{x \in [B_-, 1/2) : \tau(x) = n\}$. Then $J = \cup_{n=1}^{\infty}(I_n \cup \hat{I}_n)$, $I_1 = \{B\}$, $\hat{I}_1 = \{B_-\}$, and $|f'(x)| > 1$ for $x \in I_1 \cup \hat{I}_1$. Consider $n \geq 2$. The definition of f implies that I_n consists of finite disjoint intervals, say $J_{n,i}$'s, and f maps each interval homeomorphically onto $[B_-, B]$. By the mean value theorem, there exists a point in each of the components of $[1/2, B] \setminus I_n$ at which the absolute value of $(f^n)'$ is greater

than 1. The discontinuity points are sent to the fixed point 0 by f^2. Since $S_f < 0$, by (2.2) we have $S_{f^n} < 0$ and hence by (2.3) applied to f^n, we obtain that the absolute values of $(f^n)'$ at the end points of each interval $J_{n,j}$ are greater than 1. By (2.3) again, we have $|(f^n)'(x)| > 1$ for all $x \in I_n$. By using the same argument, we have $|(f^n)'(x)| > 1$ for all $x \in \hat{I}_n$ and the first claim follows.

Second, we claim that for every $x \in [0, 1]$ whose orbit does not go through $1/2$, there exists a positive integer n_x such that

$$|(f^{n_x})'(x)| > 1. \tag{2.5}$$

If $x \in J$, (2.5) follows (2.4) by taking $n_x = \tau(x)$. If $x \in [B_-, B] \setminus J$, $f^n(x) \notin [B_-, B]$ for all $n \geq 1$, then $|f^n(x)| > 1$ for all n sufficiently large since $|f'| > 1$ on $[0, 1] \setminus [B_-, B]$. If $x \notin [B_-, B]$, we let $n = 1$.

Third, we claim that for any nonempty open set $U \subset [0, 1]$, there exists a positive integer n such that

$$f^n(U) \supset [0, 1]. \tag{2.6}$$

Let U be an interval in $[0, 1]$. There is a positive integer n and a subinterval $U_0 \subset U$ such that $f^n(U_0) \subset J$. For convenience, we define $R(x) = f^{\tau(x)}(x)$ for $x \in J$. Statement (2.4) says that R expands the lengths of intervals in J and hence there is a $k > 0$ and a subinterval $V_0 \subset f^n(U_0)$ such that $R^k(V_0)$ contains a discontinuity point of R. Thus there exists $m > 0$ such that $p \in f^m(V_0)$. Now it remains to prove that $f^{m+\ell}(V_0) = [0, 1]$ for some $\ell > 0$. Let E be the point in the interval (B, C) such that $f(E) = 0$. Since f maps $[B, E]$ homeomorphically onto $[0, B]$, there exists a unique $d \in [B, E]$ such that $f(d) = 1/2$.

Then $f^{m+2\hat{\ell}}(V_0) \supset [1/2, d]$ for some $\hat{\ell} > 0$. Thus, there exists $\hat{\ell} > 0$ such that $f^{m+2\hat{\ell}}(V_0) \supset [1/2, d]$. Since $f^2([1/2, d]) = f([1/2, 1]) = [0, 1]$, $f^{m+2\hat{\ell}+2}(V_0) \supset f^2([1/2, d]) = [0, 1]$. The proof of the third claim is complete.

Finally, we are in position to obtain the three properties of Devaney's chaos. Let U be any nonempty open interval in $[0, 1]$. Then there exist a nonempty open interval V and a closed interval W such that $V \subset W \subset U$. By Eq. (2.6), there exists a positive integer n such that $f^n(V) \supset [0, 1]$ and hence $f^n(W) \supset W$. By the fixed point theorem, f^n has a fixed point in W. Therefore, f has a periodic point in W and so in U. We have proved that the set of periodic points is dense in $[0, 1]$. Then (2.6) immediately implies that f is topologically transitive. For sensitive dependence of f, we take $\eta = \frac{1}{4}$ and let $x \in [0, 1]$ and $\epsilon > 0$ be arbitrary. Take U to be the interval $(x, x + \frac{\epsilon}{2})$ or $(x - \frac{\epsilon}{2}, x)$ provided it is well defined. By (2.6), we have $f^n(U) \supset [0, 1]$. Thus there exists $y \in U$ such that $|f^n(x) - f^n(y)| > \frac{1}{4} = \eta$. The proof of the theorem is complete. □

3. Numerical study of MLM

In this section, we present numerical experiments on MLM made by computing spectra of waveforms to observe that no chaotic window occurs and orbits form uniform distributions in $[0, 1]$. On the other hand, we compute Poincaré recurrences to verify that the MLM possesses the positive topological entropy, which shows that the MLM is a chaotic map.

3.1. Spectra of waveforms

In order to characterize the motion of MLM, we compute spectra of waveforms of the system (2.1) with different γ. The spectrum of a waveform is computed using the FFT subroutine in MATLAB and the spectrum distribution is displayed by plotting the frequency versus $\log_{10}(|\text{fft}(\cdot)|_2)$. Here the FFT subroutine is the discrete Fourier transform, sometimes called the finite Fourier transform, which is a Fourier transform widely employed in signal processing and related fields to analyze the frequencies contained in a sampled signal. Therefore, we generate a sequence from the MLM, sampling data at 1000 Hz.

Figs. 3.1 and 3.2 present attractors of (2.1) and plot the spectra of waveforms at $\gamma = 5.9$ and 10.8, respectively. Note that we observe that all attractors form uniform distributions in $[0, 1]$ at the other values of $\gamma \geq 4$. The spectra of waveforms are revealed to have contained no definite frequency in the signals [13]. Moreover, numerically speaking, there is no chaotic window for the MLM.

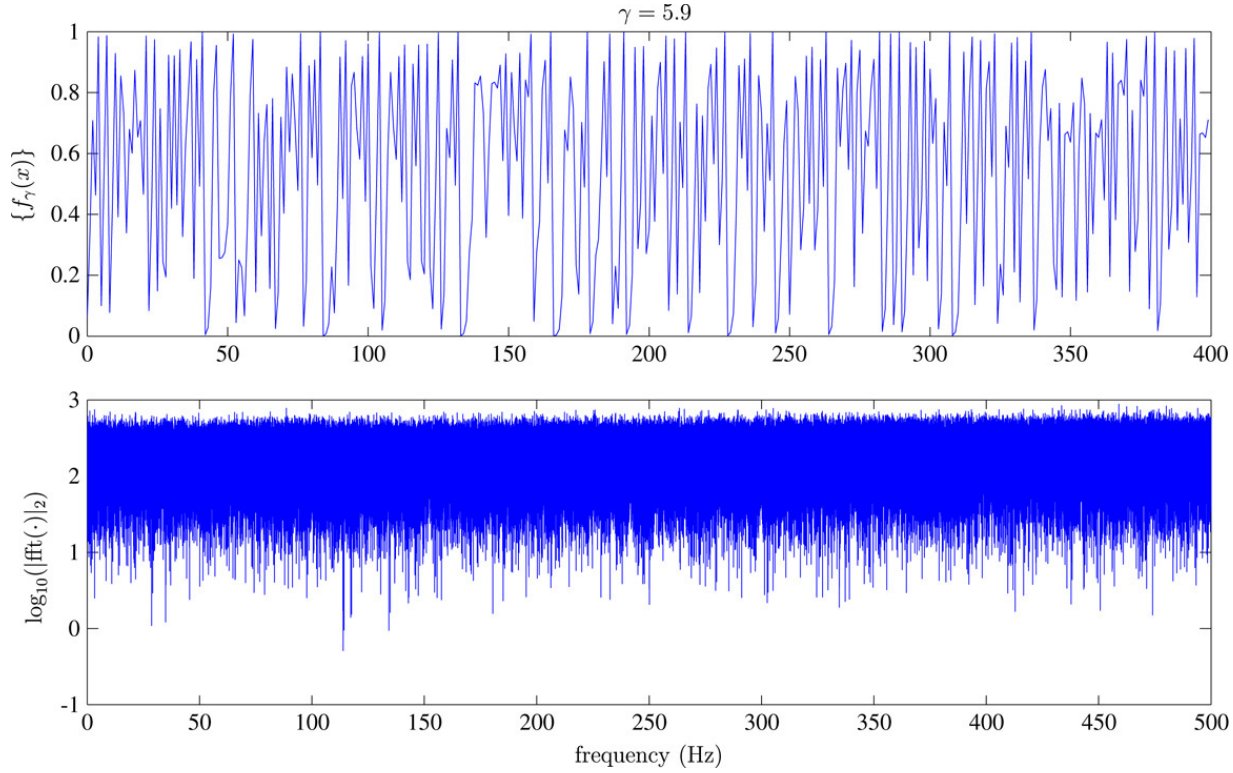

Fig. 3.1. The attractor $\{f_\gamma(x)\}$ and the spectra of waveforms of MLM for $\gamma = 5.9$.

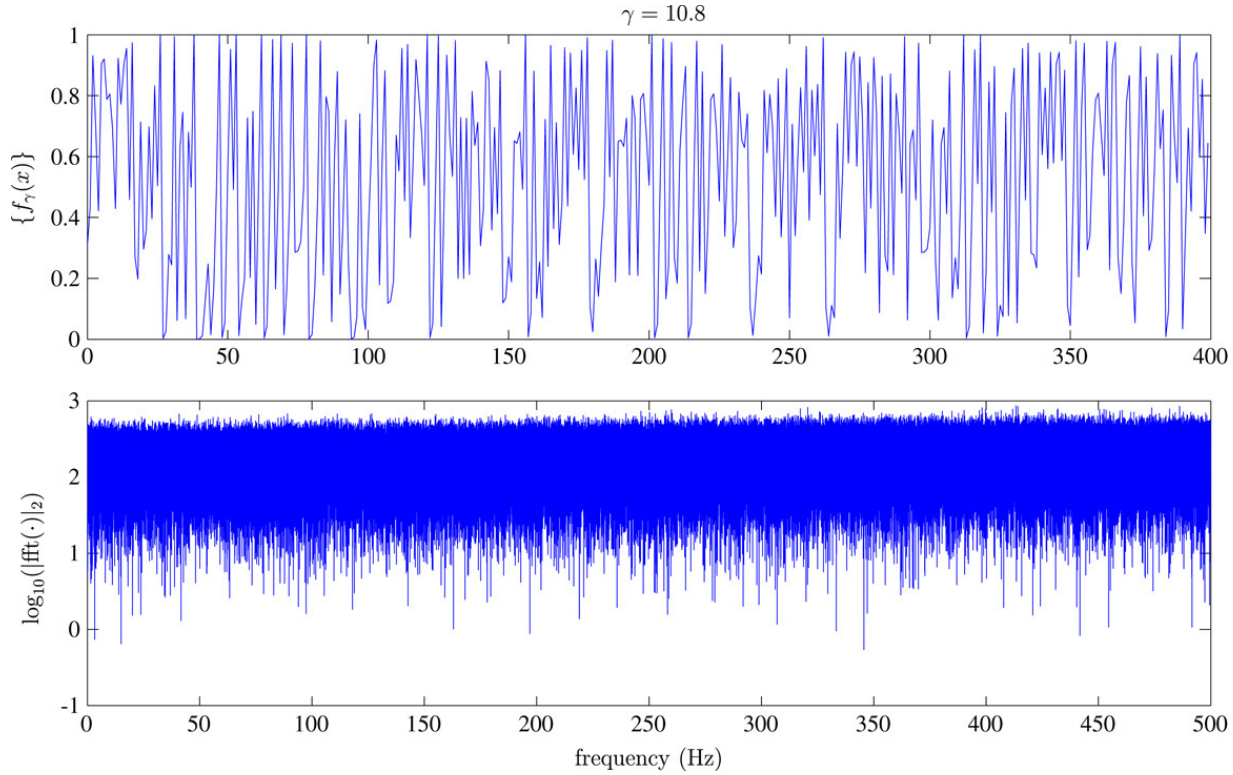

Fig. 3.2. The attractor $\{f_\gamma(x)\}$ and the spectra of waveforms of MLM for $\gamma = 10.8$.

3.2. Poincaré recurrences

We wish to briefly recall some of the definitions on the fractal dimension for Poincaré recurrences, which are main indicators and characteristics of the repetition of behavior of dynamical systems in time. We need to study the statistical properties of the quantity $\tau(x, U)$, the first return time of the orbit through x into a set U (see [22] and references therein). Typical motions in dynamical systems repeat their behavior in time. Simplicity or complexity of orbits often can be displayed in terms of Poincaré recurrences. Furthermore, Poincaré recurrences could also be used to describe what happens for the map in the regions of the phase space with regular or chaotic motions [18].

Instead of looking at the mean return time or at the return time of points, we now adopt another point of view [1]. We define the smallest possible time of return into U by taking the infimum over all return times of the points of the set. We consider a dynamical system $(\mathbb{R}^d, f)$ with f being continuous and $d \in \mathbb{N}$. Let $A \subset \mathbb{R}^d$ be an f-invariant subset. We follow the general Carathéodory construction and consider covers of A by open balls. We denote by $\mathcal{B}_\epsilon$ the class of all finite or countable open covering of A by balls of diameter less than or equal to ϵ. Let the Poincaré recurrence for an open ball $U \subset \mathbb{R}^d$ be

$$\tau(U) = \inf\{\tau(x, U) : x \in U\},$$

where $\tau(x, U) = \min\{n \in \mathbb{N} : f^n(U) \cap U \neq \emptyset\}$ is the first return time of $x \in U$. By convention, we set the return time $\tau(x, U)$ to be infinity if the point x never comes back to U. Given $\mathcal{C} \in \mathcal{B}_\epsilon$ and $\alpha, q \in \mathbb{R}$, we consider the sum

$$\mathcal{M}(\alpha, q, \epsilon, \mathcal{C}) = \sum_{U \in \mathcal{C}} \exp(-q\tau(U))|U|^\alpha, \tag{3.1}$$

where $|U|$ stands for the diameter of the set U. Now, define

$$\mathcal{M}(\alpha, q, \epsilon) = \inf\{\mathcal{M}(\alpha, q, \epsilon, \mathcal{C}) : \mathcal{C} \in \mathcal{B}_\epsilon\}.$$

The limit

$$M(\alpha, q) = \lim_{\epsilon \to 0} \mathcal{M}(\alpha, q, \epsilon)$$

has an abrupt change from infinity to zero as, for a fixed q, one varies α from zero to infinity. The transition point defines a function $\alpha_c(q)$ as follows:

$$\alpha_c(q) = \inf\{\alpha : M(\alpha, q) = 0\}.$$

This function is said to be the *spectrum of dimensions for Poincaré recurrences*. Moreover, we let $q_0 := \sup\{q : \alpha_c(q) > 0\}$. Then, roughly speaking, q_0 is the smallest solution of the equation $\alpha(q) = 0$. The number q_0 is called the *dimension for Poincaré recurrences* (see [3] and references therein).

For computational purposes [2], we shall derive an asymptotic relation between $\tau(U)$, $\ln\epsilon$ and q_0. For the sake of simplicity, we assume that $M(\alpha_c(q), q)$ is a finite number. Then the partition function (3.1) behaves as follows:

$$\mathcal{M}(\alpha_c(q), q, \epsilon, \mathcal{C}) = \sum_{U \in \mathcal{C}} \exp(-q\tau(U))|U|^{\alpha_c(q)} \sim 1,$$

i.e.,

$$\frac{1}{N} \sum_{U \in \mathcal{C}} \exp(-q\tau(U))|U|^{\alpha_c(q)} \sim \frac{1}{N}, \tag{3.2}$$

where N is the number of elements in the cover $\mathcal{C}$. But we know that if ϵ is small enough then $1/N$ behaves like ϵ^b, where b is the box dimension of the set A (provided that it exists and is equal to the Hausdorff dimension [16]).

Therefore, we may rewrite the asymptotic equality (3.2) as follows:

$$\langle \exp(-q\tau(U))|U|^{\alpha_c(q)} \rangle \sim \epsilon^b,$$

where the brackets $\langle \cdot \rangle$ denote the mean value. For $q = q_0$, we have

$$\langle \exp(-q\tau(U)) \rangle \sim \epsilon^b. \tag{3.3}$$

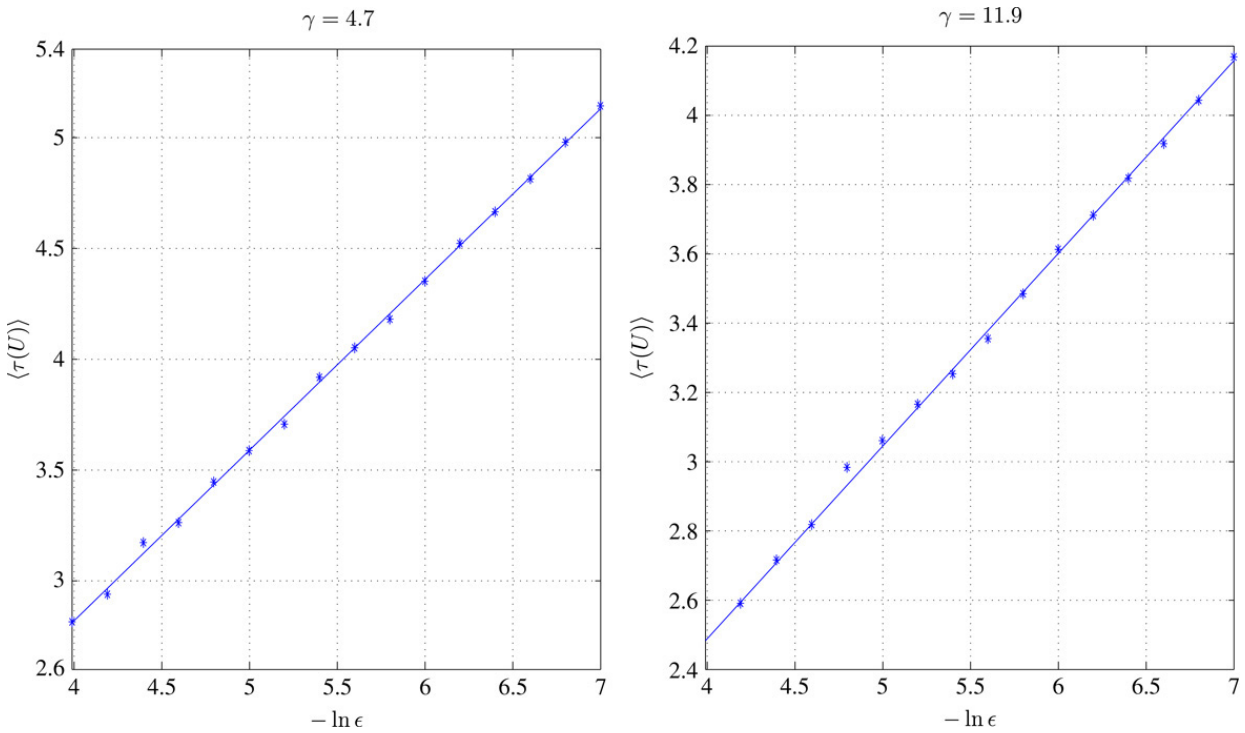

Fig. 3.3. Poincaré recurrences of MLM for $\gamma = 4.7$ and 11.9 with respect to the slopes 0.77 and 0.57, respectively. The dispersion of the calculated values of the slopes is about 3%.

Here (3.3) can be treated as the definition of the dimension q_0 for Poincaré recurrences.

If (3.3) is satisfied, we may expect the average value $\langle \tau(U) \rangle$ for Poincaré recurrences to satisfy the following asymptotic equality:

$$\langle \tau(U) \rangle \sim \frac{b}{q_0}(-\ln \epsilon), \tag{3.4}$$

where $|U| \leq \epsilon$ and $\epsilon \ll 1$. Our numerical simulations later will confirm this conjecture, plotting $\langle \tau(U) \rangle$ versus $(-\ln \epsilon)$ and evaluating the slope $\frac{b}{q_0}$.

Furthermore, the relation in (3.4) implies that the dynamical system $(\mathbb{R}^d, f)$ possesses positive topological entropy [3]. On the other hand, in [20], it was proved that the Lyapunov exponent of some class of f can be estimated from the behavior of the first return times of a ball as the diameter vanishes. More precisely, if f is a piecewise monotonic mapping with a derivative of bound p-variation for some $p > 0$ and if μ is an ergodic f-invariant measure with non-zero entropy, then for μ-almost every x, we have

$$\lambda_\mu \geq \left(\lim_{\epsilon \to 0} \frac{\tau(x, U)}{-\ln \epsilon} \right)^{-1}, \tag{3.5}$$

where λ_μ is the Lyapunov exponent of an invariant measure μ. Hence, from (3.4) and (3.5), if the slope $\frac{b}{q_0}$ is positive, it implies that the map f has a positive Lyapunov exponent.

Remark. For a function $f : [0, 1] \to \mathbb{R}$ and $p > 0$, we define the p-variation of f by

$$\mathrm{var}_p(f) := \sup \left\{ \sum_{i=1}^{N-1} |f(x_{i+1}) - f(x_i)|^p \right\},$$

where the supremum is taken along all finite ordered sequences of points $0 \leq x_1 < x_2 < \cdots < x_N \leq 1$ and integers N.

Fig. 3.3 plots Poincaré recurrences of the system (2.1) with $\gamma = 4.7$ and 11.9. The plot of $\langle \tau(U) \rangle$ versus $(-\ln \epsilon)$ has the positive slopes 0.77 and 0.57, respectively. The dispersion of the calculated values of the slopes is about 3%.

4. Synchronization in a modified logistic hyper-chaotic system

In Sections 2 and 3, from the theoretical and numerical points of view, we have shown that the MLM is a chaotic map which has no window and is uniformly distributed in [0, 1]. These fine properties are essential in the application to secure communication. In order to conform to a high standard of secure communication [21], based on MLMs in (2.1), we construct a multi-system $\mathcal{F}$, called the Modified Logistic Hyper-Chaotic System (MLHCS), defined by

$$\mathcal{F}(\mathbf{r}, \mathbf{x}, \mathbf{C}) := \mathbf{C}\begin{bmatrix} f_{\gamma_1}(x_1) \\ f_{\gamma_2}(x_2) \end{bmatrix}, \quad \mathbf{C} = \begin{bmatrix} 1-c_1 & c_1 \\ c_2 & 1-c_2 \end{bmatrix},$$

where $\mathbf{x} = [x_1, x_2]^\top$, $\mathbf{r} = [\gamma_1, \gamma_2]^\top$ and $\mathbf{C}$ is a coupling matrix with coupling strengths $c_1, c_2 \in [0, 1]$. Note that being a hyper-chaotic system [19] means that it has at least two positive Lyapunov exponents [12]. When γ_1 and γ_2 are arbitrarily chosen to be larger than 4 together with c_1 and c_2 being arbitrarily chosen between 0 and 1, there is no doubt that the resulting MLHCS could almost be a hyper-chaotic system.

Let $\mathcal{G}$ be another MLHCS defined by

$$\mathcal{G}(\mathbf{r}, \mathbf{y}, \mathbf{C}) := \mathbf{C}\begin{bmatrix} f_{\gamma_1}(y_1) \\ f_{\gamma_2}(y_2) \end{bmatrix},$$

where $\mathbf{y} = [y_1, y_2]^\top$ and the parameters $\mathbf{r}$ and $\mathbf{C}$ are the same as in $\mathcal{F}$.

Now we want to build up a system of communication between $\mathcal{F}$ and $\mathcal{G}$, called the Transmitter and Receiver, respectively. We utilize simplex partial coupling to reach synchronization between the Transmitter and Receiver. More precisely, for given initial datum $x_1^{(0)}, x_2^{(0)}, y_1^{(0)}, y_2^{(0)} \in (0, 1)$, we define the communication system (4.1) and (4.2):

$$\mathbf{x}^{(i)} = \mathcal{F}(\mathbf{r}, \mathbf{x}^{(i-1)}, \mathbf{C}), \tag{4.1}$$

$$\begin{cases} \bar{\mathbf{y}}^{(i)} = \mathcal{G}\left(\mathbf{r}, \mathbf{y}^{(i-1)}, \mathbf{C}\right), \\ \mathbf{y}^{(i)} = [x_1^{(i)}, \bar{y}_2^{(i)}]^\top, \end{cases} \tag{4.2}$$

where $\mathbf{x}^{(i)} = [x_1^{(i)}, x_2^{(i)}]^\top$ and $\bar{\mathbf{y}}^{(i)} = [\bar{y}_1^{(i)}, \bar{y}_2^{(i)}]^\top$ for $i = 1, 2, \ldots$. The vectors $\mathbf{x}^{(i)}$ and $\mathbf{y}^{(i)}$ of the Transmitter and Receiver can be synchronized by the partial portion $x_1^{(i)}$ with a suitable coupling strength $\mathbf{C}$, as i is sufficiently large. Under the usual metric on $\mathbb{R}/\mathbb{Z}$, we obtain a sufficient condition for synchronization below.

Let $|\cdot|_1$ be the usual metric on $\mathbb{R}/\mathbb{Z}$ defined by

$$|x - y|_1 = \min\{|x - y|, 1 - |x - y|\} \quad \text{for } x, y \in [0, 1).$$

For convenience, we define a function $\delta(\gamma)$,

$$\delta(\gamma) := \max_{x\in[0,1]} |f'_\gamma(x)| = \begin{cases} \gamma, & \text{if } \gamma = 4k \text{ for some } k \in \mathbb{N}, \\ \dfrac{\sqrt{\gamma^2 - 4\gamma[\frac{\gamma}{4}]}}{\frac{\gamma}{4} \pmod 1}, & \text{if } \gamma \notin \mathbb{N}. \end{cases}$$

Theorem 4.1. *If* $1 - \frac{1}{\delta(\gamma_2)} < c_2 < 1$, *then* $|x_2^{(i)} - y_2^{(i)}|_1 \to 0$ *as* $i \to \infty$.

Proof. From the system (4.1) and (4.2), it holds that $|x_2^{(i)} - y_2^{(i)}|_1 = |(1 - c_2)[f_{\gamma_2}(x_2^{(i-1)}) - f_{\gamma_2}(y_2^{(i-1)})]|_1$. By the mean value theorem applied to f_{γ_2}, we have $|x_2^{(i)} - y_2^{(i)}|_1 \le \alpha|x_2^{(i-1)} - y_2^{(i-1)}|_1 = \alpha^i|x_2^{(0)} - y_2^{(0)}|_1$, where $\alpha = (1-c_2)|f'_{\gamma_2}(\xi)|$ and $\xi \in (0, 1)$. Since $1 - \frac{1}{\delta(\gamma_2)} < c_2 < 1$, this implies that $0 < \alpha < 1$ and then $|x_2^{(i)} - y_2^{(i)}|_1 \to 0$ as $i \to \infty$. □

With Theorem 4.1, we understand that both sides of the communication system (4.1) and (4.2) can approach the same state under the chord norm. However, by using the Euclidean norm, $x_2^{(i)}$ and $y_2^{(i)}$ can only be shown to be sufficiently close for some i.

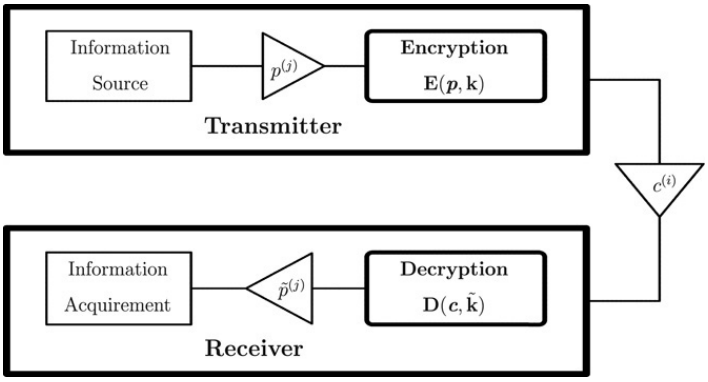

Fig. 5.1. Communication scheme.

Theorem 4.2. *Given any small* $\epsilon > 0$, *if* $|x_2^{(0)} - y_2^{(0)}|_1 < \epsilon$ *and* $1 - \frac{1}{\delta(\gamma_2)} < c_2 < 1$, *then there exists a positive integer* i *such that* $|x_2^{(i)} - y_2^{(i)}| < \epsilon$.

Proof. It follows from Theorem 4.1. □

Since there exist jumps (discontinuous points) in the MLM, we obtain an equivocal phenomenon in the proof of Theorem 4.2. By using the chord norm, $|x_2^{(i)} - y_2^{(i)}|_1$ can always be reduced when i increases under some convergence condition of c_2. However, by using Euclidean norm, $x_2^{(i)}$ and $y_2^{(i)}$ may be separated for some i and then $|x_2^{(i)} - y_2^{(i)}|$ is far away from zero which cannot be applied to secure communication.

From Theorem 4.1, we conclude that the communication system (4.1) and (4.2) can achieve synchronization of $x_2^{(i)}$ and $y_2^{(i)}$ in the chord norm. As discussed above, $x_2^{(i)}$ and $y_2^{(i)}$ can be separated far apart by using Euclidean norm, provided that $x_2^{(0)}$ and $y_2^{(0)}$ are very close, but are on the left and right hand sides of a jump point, respectively. Namely, non-synchronization can happen after some iterations. Hence, in order to guarantee synchronization under the Euclidean norm, we have to set up $x_2^{(i)}$ and $y_2^{(i)}$ to be on the same side of the jump point as they approach. After this setting and from Theorem 4.2, it is clear that $\lim_{i\to\infty} |x_2^{(i)} - y_2^{(i)}| = 0$; that is, $x_2^{(i)}$ and $y_2^{(i)}$ can reach synchronization.

5. Application in a secure communication system

In this section, we propose a secure communication system, called Asymptotic Synchronization of the Modified Logistic Hyper-Chaotic System (ASMLHCS), which is based on the communication system (4.1) and (4.2). ASMLHCS utilizes an important property of the communication system (4.1) and (4.2); that is, the Transmitter and Receiver can realize synchronization. In the ASMLHCS, there are two phases — the asymptotical synchronization phase and the encryption/decryption phase. First, we need to make both sides (the Transmitter and Receiver) carry out asymptotic synchronization. We then utilize asymptotic synchronization to accomplish the secure communication.

The communication scheme is sketched in Fig. 5.1. Information is transmitted by the Transmitter through the channel after encryption. The Receiver recovers the information by decryption.

5.1. Crypto-communication system

In this subsection, we present a crypto-communication system, the Asymptotic Synchronization of the Modified Logistic Hyper-Chaotic System (ASMLHCS), which consists of the Transmitter (5.1), (5.2) and the Receiver (5.3)–(5.5). For $i > 0$ and given $x_1^{(0)}, x_2^{(0)}, y_1^{(0)}, y_2^{(0)} \in (0, 1)$,

$$\mathbf{x}^{(i)} = \mathcal{F}(\mathbf{r}, \mathbf{x}^{(i-1)}, \mathbf{C}), \tag{5.1}$$

$$k^{(i)} = \left\lfloor x_1^{(i)} \right\rfloor_n, \tag{5.2}$$

where $k^{(i)}$ is a encrypting sequence and $\lfloor x \rfloor_n := \hat{x}$ denotes the chopped finite n digits approximation with respect to x; i.e., $|x - \hat{x}| < 10^{-n}$, $n \in \mathbb{N}$.

$$\bar{\mathbf{y}}^{(i)} = \mathcal{G}\left(\mathbf{r}, \mathbf{y}^{(i-1)}, \mathbf{C}\right), \tag{5.3}$$

$$\tilde{k}^{(i)} = \left\lfloor \bar{y}_1^{(i)} \right\rfloor_n, \tag{5.4}$$

$$\mathbf{y}^{(i)} = [k^{(i)}, \bar{y_2}^{(i)}]^\top, \tag{5.5}$$

where $\tilde{k}^{(i)}$ is a decrypting sequence of receiver.

Remark. In (5.2), $k^{(i)}$ has to be carefully picked out, either $\left\lfloor x_1^{(i)} \right\rfloor_n$ or $\left\lfloor x_1^{(i)} \right\rfloor_n + 10^{-n}$, when the interval $\left(\left\lfloor x_1^{(i)} \right\rfloor_n, \left\lfloor x_1^{(i)} \right\rfloor_n + 10^{-n}\right)$ contains one of discontinuous points of MLM. Here $k^{(i)}$ needs to be chosen on the same side as $x_1^{(i)}$ with respect to the discontinuous point. This same tactic is also applied to $x_2^{(i)}$ and $y_2^{(i)}$ of $\mathcal{F}$ and $\mathcal{G}$, respectively.

5.2. Asymptotic synchronization phase

In order to achieve secure communication, the ASMLHCS has to connect and synchronize between the Transmitter and Receiver. We use simplex direction from the Transmitter (to the Receiver) to employ a partial system of $\mathcal{F}$, $x_1^{(i)}$, to drive the system $\mathcal{G}$ in the Receiver. This is called *simplex partial driving* and it makes both sides carry out asymptotic synchronization. In this subsection, we need to estimate the number of iterations to reach asymptotic synchronization.

Let $\{x_1^{(0)}, x_2^{(0)}\}$ and $\{y_1^{(0)}, y_2^{(0)}\}$ be the initial values of $\mathcal{F}$ and $\mathcal{G}$, respectively. The ASMLHCS begins transmitting with the simplex and partial system of $\mathbf{x}^{(i)}$, and should be in asymptotic synchronization before information transmission; that is, the sequences $k^{(i)}$ and $\tilde{k}^{(i)}$ are asymptotically synchronized.

Theorem 5.1. *Using suitable tactics as indicated by the Remark in Section 5.1 for the system (5.1)–(5.5) with* $1 - \frac{1}{\delta(\gamma_2)} < c_2 < 1$, *there exists* $i_{\text{syn}} \in \mathbb{N}$ *such that*

$$\left| y_2^{(i)} - x_2^{(i)} \right| < \left[1 + \frac{c_2\delta(\gamma_1)}{1 - (1 - c_2)\delta(\gamma_2)}\right] 10^{-n}$$

as $i > i_{\text{syn}}$.

Proof. From Theorem 4.1, we know that $|x_2^{(i)} - y_2^{(i)}|_1$ can be smaller than any given tolerance when i is large enough. From the proof of Theorem 4.2, we also observe that $|x_2^{(i)} - y_2^{(i)}|$ could always be smaller than any given tolerance when $x_2^{(i)}$ and $y_2^{(i)}$ are located on same side of the jump η when $x_2^{(i)}, y_2^{(i)} \in (\eta - \theta, \eta + \theta)$, where θ is a small length dictated by this tactic. Therefore, in the system (5.1)–(5.5), we have that

$$\begin{aligned}
|x_2^{(i)} - y_2^{(i)}| &= \left|(1 - c_2)\left[f_{\gamma_2}(x_2^{(i-1)}) - f_{\gamma_2}(y_2^{(i-1)})\right] + c_2\left[f_{\gamma_1}(x_1^{(i-1)}) - f_{\gamma_1}(y_1^{(i-1)})\right]\right| \\
&< (1 - c_2)\delta(\gamma_2)\left|x_2^{(i-1)} - y_2^{(i-1)}\right| + c_2\delta(\gamma_1)\cdot 10^{-n} \quad [\text{let } \alpha = (1 - c_2)\delta(\gamma_2) \text{ and } \beta = c_2\delta(\gamma_1)] \\
&\le \alpha\left[\alpha|x_2^{(i-2)} - y_2^{(i-2)}| + \beta\cdot 10^{-n}\right] + \beta\cdot 10^{-n} \\
&\;\;\vdots \\
&\le \alpha^i|x_2^{(0)} - y_2^{(0)}| + [\alpha^{i-1} + \cdots + \alpha + 1]\beta\cdot 10^{-n}.
\end{aligned}$$

Since $1 - \frac{1}{\delta(\gamma_2)} < c_2 < 1$, $0 < \alpha < 1$, and $|x_2^{(i)} - y_2^{(i)}| < (1 + \frac{\beta}{1-\alpha})10^{-n}$ for $i > i_{\text{syn}}$ as $\alpha^{i_{\text{syn}}} < 10^{-n}$. □

After i_{syn} steps of transmission, both sides of the Transmitter and Receiver reach hyper-chaotic asymptotic synchronization. In the next subsection, we utilize the synchronized system to encrypt a plaintext $\boldsymbol{p}$ to a ciphertext $\boldsymbol{c}$ in the Transmitter and to decrypt $\boldsymbol{c}$ to $\tilde{\boldsymbol{p}}$ in the Receiver. Obviously, $\tilde{\boldsymbol{p}}$ equals $\boldsymbol{p}$.

5.3. Encryption and decryption phase

After reaching asymptotic synchronization, ASMLHCS starts utilizing $k^{(i)}$ to mask the plaintext into the ciphertext.

Theorem 5.2. *For $j \geq 1$ and $i = i_{\text{syn}} + j$, then*

$$\left|y_1^{(i)} - x_1^{(i)}\right| < \left[(1-c_1)\delta(\gamma_1) + c_1\delta(\gamma_2) + \frac{c_1c_2\delta(\gamma_1)\delta(\gamma_2)}{1-(1-c_2)\delta(\gamma_2)}\right]10^{-n}.$$

Proof.

$$\begin{aligned}\left|y_1^{(i)} - x_1^{(i)}\right| &= \left|(1-c_1)\left[f_{\gamma_1}(y_1^{(i-1)}) - f_{\gamma_1}(x_1^{(i-1)})\right] + c_1\left[f_{\gamma_2}(y_2^{(i-1)}) - f_{\gamma_2}(x_2^{(i-1)})\right]\right| \\ &< (1-c_1)\delta(\gamma_1)\cdot 10^{-n} + c_1\delta(\gamma_2)|y_2^{(i-1)} - x_2^{(i-1)}| \\ &< \left[(1-c_1)\delta(\gamma_1) + c_1\delta(\gamma_2) + \frac{c_1c_2\delta(\gamma_1)\delta(\gamma_2)}{1-(1-c_2)\delta(\gamma_2)}\right]10^{-n}. \quad \text{(by Theorem 5.1).} \quad \square\end{aligned}$$

In the Transmitter:
Given $m \in \mathbb{N}$ and $m < n-1$ such that

$$\left[(1-c_1)\delta(\gamma_1) + c_1\delta(\gamma_2) + \frac{c_1c_2\delta(\gamma_1)\delta(\gamma_2)}{1-(1-c_2)\delta(\gamma_2)}\right]10^{-n} < \frac{1}{2}\times 10^{-m},$$

and for $j \geq 1$ and $i = i_{\text{syn}} + j$, the plaintext $\boldsymbol{p}$ is decomposed into the integer sequence $\{p^{(i)}\}$ and each integer is small than 10^m. The encryption $\mathbf{E}(\boldsymbol{p}, \mathbf{k})$ is

$$c^{(i)} = k^{(i)} + p^{(j)} \times 10^{-m},$$

where $c^{(i)}$ is the ciphertext and $\mathbf{c} = \{c^{(i)}\}$.

Before transmitting the ciphertext $c^{(i)}$ to the corresponding connection point, we can make additional encoding before sending $c^{(i)}$. Similarly, after obtaining $c^{(i)}$, the Receiver has to remove any such additional encoding before the decrypting process.

In the Receiver:
There are two important procedures — the decryption and the *implicit driving*. For $j \geq 1$ and $i = i_{\text{syn}} + j$, the decryption $\mathbf{D}(\mathbf{c}, \tilde{\mathbf{k}})$ is

$$\tilde{p}^{(j)} = \lceil c^{(i)} - \tilde{k}^{(i)} \rceil_m \times 10^m,$$

where $\lceil x \rceil_m := \hat{x}$ denotes the rounded m-digit approximation to x, i.e., $|x - \hat{x}| < \frac{1}{2}\times 10^{-m}$. On the other hand, we have to maintain the asymptotical synchronization of both sides as the successive steps in ASMLHCS. Here we propose *implicit driving* to make $k^{(i)}$ and $\tilde{k}^{(i)}$ preserve the asymptotic synchronization in the encryption/decryption phase; that is, (5.5) is replaced by

$$\mathbf{y}^{(i)} = [k^{(i)} - \tilde{p}^{(j)} \times 10^{-m}, \bar{y_2}^{(i)}]^\top.$$

Remark. Given $x_1^{(0)}, x_2^{(0)}, y_1^{(0)}, y_2^{(0)}$ with $c_1, c_2 \in (0,1)$ and $\gamma_1, \gamma_2 \in (4, \infty)$. For $i \geq 1$, we have $x_1^{(i)}, x_2^{(i)}, \bar{y}_1^{(i)}, \bar{y}_2^{(i)}$, $y_1^{(i)}, y_2^{(i)}, k^{(i)}, \tilde{k}^{(i)} \in (0,1)$ and $c^{(i)} \in (0,2)$.

In this section, we present the ASMLHCS and prove that it can be synchronized in the asymptotic synchronization phase. The system is always kept synchronized by implicit driving in the encryption/decryption phase. For simplicity, we have presented our work in the decimal system. It should be pointed out that the same work can easily be realized in the hexadecimal system as well.

6. Conclusion

In conclusion, we show a robust chaotic map, the Modified Logistic Map, which not only exhibits no window but is also uniformly distributed in [0, 1]. On the basis of this map, we design a multi-system hyper-chaotic synchronization system, the Asymptotic Synchronization of the Modified Logistic Hyper-Chaotic System, for secure communication. The system can achieve, theoretically, asymptotical synchronization between the Transmitter and Receiver after finite times in simplex partial coupling transmission. Furthermore, the implicit driving technique always guarantees asymptotical synchronization between the drive and response systems during the plaintext transmission.

Acknowledgments

This research was supported in part by the National Science Council and the National Center for Theoretical Sciences, Taiwan. We would like to thank Mr. Shih-Liang Chen for providing us with many references and helpful discussions.

References

[1] V. Afraimovich, J.R. Chazottes, B. Saussol, Pointwise dimensions for Poincaré recurrences associated with maps and special flows, Discrete Contin. Dyn. Syst. 9 (2) (2003) 263–280.
[2] V. Afraimovich, W.W. Lin, N.F. Rulkov, Fractal dimension for Poincaré recurrences as an indicator of synchronized chaotic regimes, Internat. J. Bifur. Chaos Appl. Sci. Engrg. 10 (10) (2000) 2323–2337.
[3] V. Afraimovich, J. Schmeling, E. Ugalde, J. Urías, Spectra of dimensions for Poincaré recurrences, Discrete Contin. Dyn. Syst. 6 (4) (2000) 901–914.
[4] E. Barreto, B.R. Hunt, C. Grebogi, J.A. Yorke, From high dimensional chaos to stable periodic orbits: The structure of parameter space, Phys. Rev. Lett. 78 (24) (1997) 4561–4564. This is true not only for low-dimensional systems, but also for high-dimensional chaotic systems.
[5] D.K. Campbell, An introduction to nonlinear dynamics, in: Daniel L. Stein (Ed.), Lectures in the Sciences of Complexity, 1989, pp. 3–105.
[6] R.L. Devaney, An Introduction to Chaotic Dynamical Systems, 2nd edition, Addison-Wesley, Redwood City, CA, 1989.
[7] D. Gulick, Encounters with Chaos, McGraw-Hill, New York, 1992.
[8] G. Heidari-Bateni, C.D. McGillem, A chaotic direct-sequence spread-spectrum communication system, IEEE Trans. Comm. 42 (1994) 1524–1527.
[9] R. Holmgren, A First Course in Discrete Dynamical Systems, 2nd edition, Springer-Verlag, New York, 1996.
[10] K. Klomkarn, A. Jansri, P. Sooraksa, A design of stream cipher based on multi-chaotic functions, in: IEEE Int. Symp. Communications and Information Technology, vol. 2, 2004, pp. 26–29.
[11] R.L. Kraft, Chaos, cantor sets, and hyperbolicity for the logistic maps, Amer. Math. Monthly 106 (5) (1999) 400–408.
[12] E. Ott, An Equation for Hyperchaos, Cambridge University Press, Cambridge, 1993.
[13] T.S. Parker, L.O. Chua, Practical Numerical Algorithms for Chaotic Systems, Springer-Verlag, New York, 1989.
[14] L.M. Pecora, T.L. Carroll, Synchronization in chaotic systems, Phys. Rev. Lett. 64 (8) (1990) 821–824.
[15] F. Peng, S.S. Qiu, L. Min, An image encryption algorithm based on mixed chaotic dynamic systems and external keys, in: International Conference on Communications, Circuits and Systems, vol. 2, 2005, pp. 27–30.
[16] Y.B. Pesin, Dimension Theory in Dynamical Systems: Contemporary Views and Application, The University of Chicago Press, Chicago and London, 1997, p. 304.
[17] C. Robinson, Stability, Symbolic Dynamics, and Chaos, CRC Press, Boca Raton, 1995.
[18] L. Rossi, G. Turchetti, S. Vaienti, Poincaré recurrences as a tool to investigate the statistical properties of dynamical systems with integrable and mixing components, in: International Workshop on Chaotic Transport and Complexity in Fluids and Plasmas, J. Phys. Conference Ser. 7 (2005) 94–100.
[19] O.E. Rössler, An equation for hyperchaos, Phys. Lett. A 71 (2–3) (1979) 155–157.
[20] B. Saussol, S. Troubetzkoy, S. Vaienti, Recurrence, dimensions and Lyapunov exponents, J. Statist. Phys. 106 (314) (2002) 623–634.
[21] M.I. Sobhy, A.-E.R. Shehata, Methods of attacking chaotic encryption and countermeasures, in: IEEE International Conf. on Acoustics, Speech, and Signal Processing, vol. 2, 2001, pp. 1001–1004.
[22] L.S. Young, Recurrence times and rates of mixing, Israel J. Math. 110 (1) (1999) 153–188.
[23] H. Zhou, X.T. Ling, Problems with the chaotic inverse system encryption approach, IEEE Trans. Circuits Syst. I, Fundam. Theory Appl. 44 (3) (1997) 268–271.