Chaotic Generator in Digital Secure Communication

Shu-Ming Chang *

Abstract—**A chaotic orbit generated by a nonlinear system is irregular, aperiodic, unpredictable and has sensitive dependence on initial conditions. However, the chaotic trajectory is still not well enough to be a crypto system in digital secure communication. Therefore, 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. Based on the MLMs, we establish a Modified Logistic Hyper-Chaotic System (MLHCS) and apply MLHCS to develop a symmetric cryptography algorithm, Asymptotic Synchronization of Modified Logistic Hyper-Chaotic System (ASMLHCS).**

Keywords: modified logistic map, digital secure communication, no window, hyper-chaos, chaotic encryption

1 Introduction

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 $3.57 < \gamma \leq 4$ [7, 8, 10]. 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, logistic map is also proved to be chaotic on an invariant Cantor set for all $\gamma > 4$ which is unstable [12, 18].

Pecora and Carrol [15] have shown that a chaotic system (respond 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 masking streams to carry information which can be recovered by chaotic synchronization behavior between the transmitter (drive system) and receiver (respond system). Sobhy and Shehata [22] 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 in enhancing the complexity of the output sequence. Heidari-Bateni and McGillem [9] use a chaotic map to initialize another chaotic map. Utilizing a multi-system with serval chaotic maps are switched by the specific mechanism [11] or combined into a chaotic system chain [24]. Peng et al. [16] combine the above two approaches.

In this paper, we propose a robust map, 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. Basing on two MLMs, we establish a Modified Logistic Hyper-Chaotic System (MLHCS). We then develop a symmetric cryptography algorithm, Asymptotic Synchronization of Modified Logistic Hyper-Chaotic System (ASMLHCS), consisting of two MLHCSs. There are two parts in the ASMLHCS, namely the asymptotic synchronization phase and the Encrtyption/Decryption phase. The details will be introduced in later sections.

2 Modified Logistic Map (MLM)

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

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

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 $\gamma \leq 4$, 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 $3.57 < \gamma \leq 4$. Consequently, the sequence generated by the MLM never settles down to a fixed point

*Department of Applied Mathematics, National Chiao Tung University, Hsinchu, 300, Taiwan. This research was supported in part by the National Science Council, NSC 97-2115-M-009-003-MY2 and the National Center for Theoretical Sciences, Taiwan. Email: smchang@math.nctu.edu.tw

ISBN:978-988-18210-1-0

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 one. In fact, the attractor of a chaotic window visually forms periodic points which has been proved to be open and dense.

As the MLM has no chaotic windows for $\gamma < 4$ which is suitable as a chaotic mask in secure communication, in the following we shall show that the MLM has also chaotic behavior according to Devaney's definition [7] for $\gamma \geq 4$. In these cases the lengths of strange attractors are always one 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.

Theorem 2.1. [6] *If $\gamma \geq 4$, then f_γ exhibits Devaney's chaos on* $[0, 1]$.

3 Numerical study of MLM

In this section, we present the numerical experiments on MLM 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, 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 1,000 Hz.

Figures 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 revealed to have contained no definite frequency in the signals [14]. Moreover, numerically speaking, there is no chaotic window for the MLM.

3.2 Poincaré recurrences

Poincaré recurrences are main indicators and characteristics of the repetition of behavior of dynamical systems

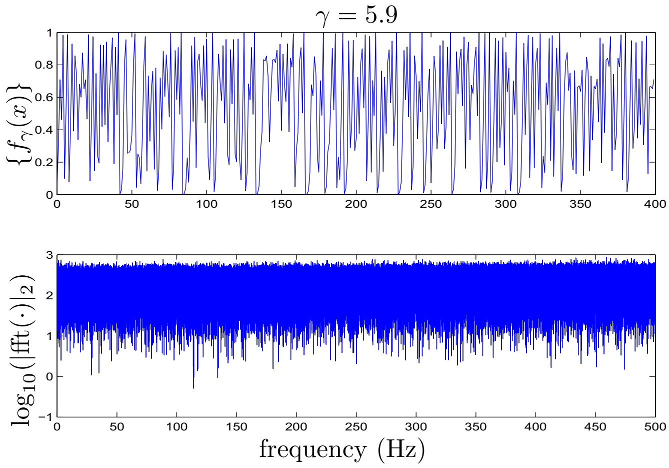

Figure 3.1: The attractor $\{f_\gamma(x)\}$ and the spectra of waveforms of MLM for $\gamma = 5.9$.

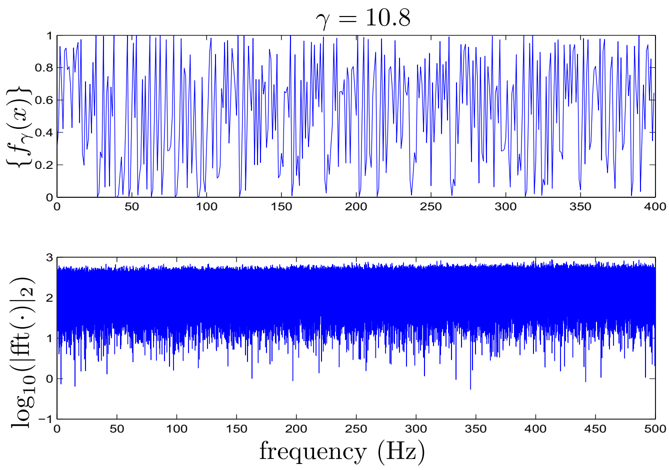

Figure 3.2: The attractor $\{f_\gamma(x)\}$ and the spectra of waveforms of MLM for $\gamma = 10.8$.

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 [23] 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 to describe what happens for the map in the regions of the phase space with regular or chaotic motions [19].

Instead of looking at the mean return time or at the return time of points, we now adopt another point of view. We define the smallest possible return time into U by taking the infimum over all return times of the points of the set [6]. 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.

ISBN:978-988-18210-1-0

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

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

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.,

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

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 [17]).

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

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

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 that the average value $\langle \tau(U) \rangle$ for Poincaré recurrences satisfies the following asymptotic equality

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

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 [21], 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

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

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.

Figure 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 %.

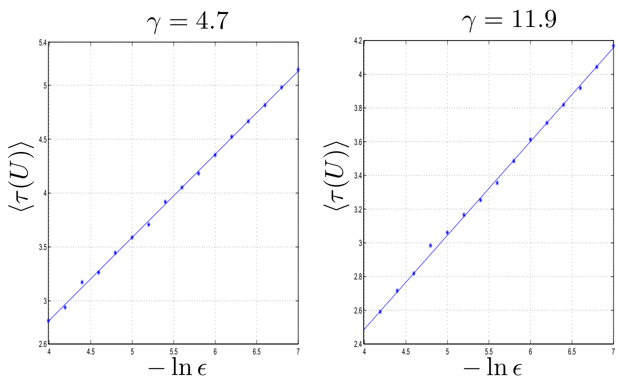

Figure 3.3: Poincaré recurrences of MLM for $\gamma = 4.7$ and 11.9 with respect to the slopes 0.77 and 0.57, respectively. The dispersion of the calculated values of the slopes is about 3 %.

4 Synchronization in modified logistic hyper-chaotic system

In Sections 2 and 3, from the theoretical and numerical points of view, we have shown that MLM is a chaotic map which has no window and is uniformly distributed

ISBN:978-988-18210-1-0

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 [22], 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 a hyper-chaotic system [20] means that it has at least two positive Lyapunov exponents [13]. When γ_1 and γ_2 are arbitrary chosen to be larger than 4 together with c_1 and c_2 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 communication system 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)–(4.2):

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

$$\left\{ \begin{array}{rcl} \bar{\mathbf{y}}^{(i)} & = & \mathcal{G}\left(\mathbf{r},\mathbf{y}^{(i-1)},\mathbf{C}\right), \\ \mathbf{y}^{(i)} & = & [x_1^{(i)}, \bar{y_2}^{(i)}]^\top, \end{array} \right. \tag{4.2}$$

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

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

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

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

where $k \in \mathbb{N}$.

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

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

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* $|x_2^{(i)} - y_2^{(i)}| < \epsilon$.

5 Application in secure communication system

In this section, we propose a secure communication system, called Asymptotic Synchronization of Modified Logistic Hyper-Chaotic System (ASMLHCS), which is based on the communication system (4.1)–(4.2). ASMLHCS utilizes an important property of the communication system (4.1)–(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 Figure 5.1. Information is transmitted by the Transmitter through the channel after Encryption. The Receiver recovers the information by Decryption.

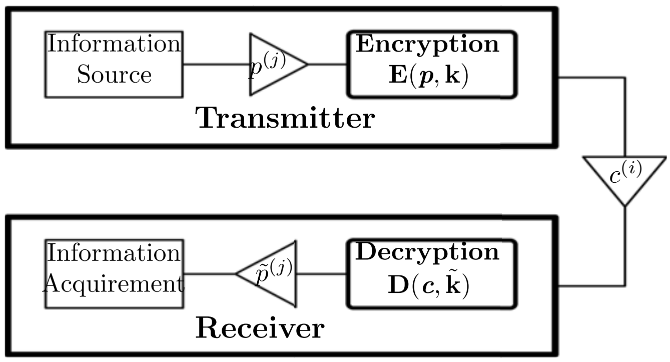

Figure 5.1: Communication scheme.

6 Conclusions

In conclusion, we show a robust chaotic map, the Modified Logistic Map, which not only exhibits no window but is also uniformly distributed in $[0,1]$. Based on this map, we design a multi-system hyper-chaotic synchronization system, the Asymptotic Synchronization of 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 respond systems during the plaintext transmission.

References

[1] V. Afraimovich, J. R. Chazottes, and B. Saussol. Pointwise dimensions for Poincaré recurrences associated with maps and special flows. *Discrete Contin. Dyn. Syst.*, 9(2):263–280, 2003.

[2] V. Afraimovich, W. W. Lin, and N. F. Rulkov. Fractal dimension for Poincaré recurrences as an indicator of synchronized chaotic regimes. *Internat. J. Bifur. Chaos Appl. Sci. Engrg.*, 10(10):2323–2337, 2000.

[3] V. Afraimovich, J. Schmeling, E. Ugalde, and J. Urías. Spectra of dimensions for Poincaré recurrences. *Discrete Contin. Dyn. Syst.*, 6(4):901–914, 2000.

[4] E. Barreto, B. R. Hunt, C. Grebogi, and J. A. Yorke. From high dimensional chaos to stable periodic orbits: the structure of parameter space. *Phys. Rev. Lett.*, 78(24):4561–4564, 1997. This is true not only for low-dimensional systems, but also for high-dimensional chaotic systems.

[5] David K. Campbell. An introduction to nonlinear dynamics. In Daniel L. Stein, editor, *Lectures in the Sciences of Complexity*, pages 3–105, 1989.

[6] S. M. Chang, M. C. Li, and W. W. Lin. Asymptotic synchronization of modified logistic hyper-chaotic systems and its applications. *Nonlinear Analysis: Real World Applications*, 10(2):869–880, 2009.

[7] Robert L. Devaney. *An introduction to chaotic dynamical systems.* Addison-Wesley, Redwood City, CA, 2nd edition, 1989.

[8] Denny Gulick. *Encounters with chaos.* McGraw-Hill, New-York, 1992.

[9] G. Heidari-Bateni and C. D. McGillem. A chaotic direct-sequence spread-spectrum communication system. *IEEE Trans. Comm.*, 42:1524–1527, 1994.

[10] R. Holmgren. *A first course in discrete dynamical systems.* Springer-Verlag, New-York, 2nd edition, 1996.

[11] K. Klomkarn, A. Jansri, and P. Sooraksa. A design of stream cipher based on multi-chaotic functions. In *IEEE Int. Symp. Commmunications and Information Technology*, volume 2, pages 26–29, 2004.

[12] R. L. Kraft. Chaos, cantor sets, and hyperbolicity for the logistic maps. *Amer. Math. Monthly*, 106(5):400–408, 1999.

[13] E. Ott. *An equation for hyperchaos.* Cambridge University Press, Cambridge, 1993.

[14] T. S. Parker and L. O. Chua. *Practical numerical algorithms for chaotic systems.* Springer-Verlag, New-York, 1989.

[15] L. M. Pecora and T. L. Carroll. Synchronization in chaotic systems. *Phys. Rev. Lett.*, 64(8):821–824, 1990.

[16] F. Peng, S. S. Qiu, and L. Min. An image encryption algorithm based on mixed chaotic dynamic systems and external keys. In *International Conference on Communications, Circuits and Systems*, volume 2, pages 27–30, 2005.

[17] Y. B. Pesin. *Dimension theory in dynamical systems: contemporary views and application.* The University of Chicago Press, Chicago and London, 1997. p. 304.

[18] C. Robinson. *Stability, symbolic dynamics, and chaos.* CRC Press, Boca Raton, 1995.

[19] L. Rossi, G. Turchetti, and S. Vaienti. Poincaré recurrences as a tool to investigate the statical properties of dynamical systems with integrable and mixing compotns. In *International Workshop on Chaotic Transport and Complexity in Fluids and Plasmas*, pages 94–100. Journal of Physics: Conference Series 7, 2005.

[20] O. E. Rössler. An equation for hyperchaos. *Phys. Lett. A*, 71(2-3):155–157, 1979.

[21] B. Saussol, S. Troubetzkoy, and S. Vaienti. Recurrence, dimensions and Lyapunov exponents. *J. Statist. Phys.*, 106(314):623–634, 2002.

[22] M. I. Sobhy and A.-E. R. Shehata. Methods of attacking chaotic encryption and countermeasures. In *IEEE International Conf. on Acoustics, Speech, and Signal Processing*, volume 2, pages 1001–1004, 2001.

[23] L. S. Young. Recurrence times and rates of mixing. *Israel J. of Math.*, 110(1):153–188, 1999.

[24] H. Zhou and X. T. Ling. Problems with the chaotic inverse system encryption approach. *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, 44(3):268–271, 1997.